Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Sous-direction assistance, conseil et expertise
Bureau assistance et conseil

EBIOS 2010

ETUDE DE CAS : SECURITE D'UN SERVICE DU CLOUD

Version du 20 juillet 2011

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante (voir formulaire de recueil de commentaires en fin de guide) :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Sous-direction assistance, conseil et expertise
Bureau assistance et conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

ebios@ssi.gouv.fr

Historique des modifications

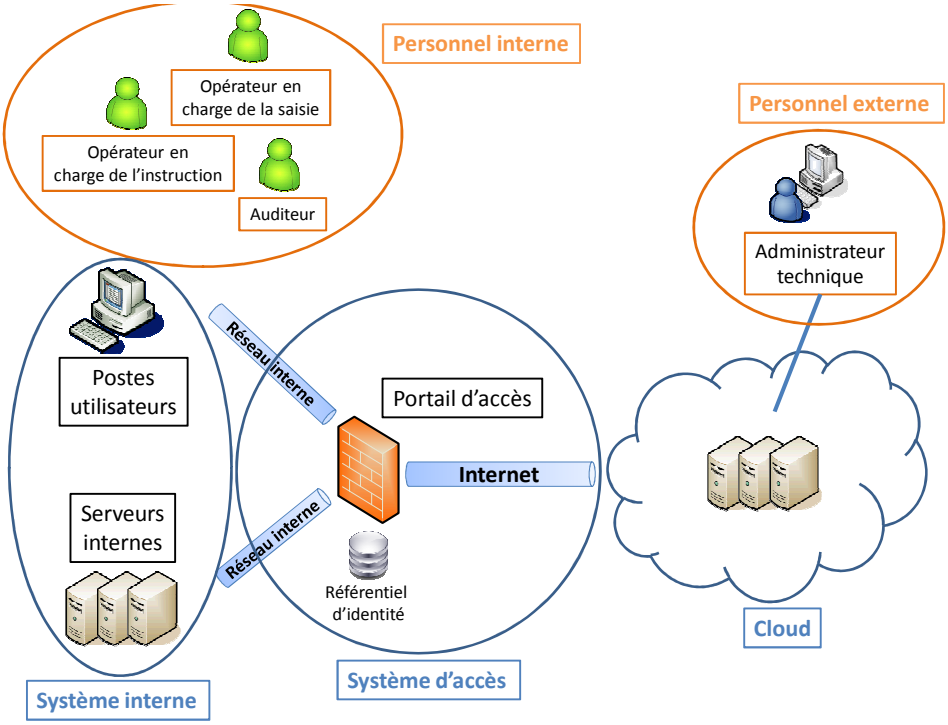
Date	Objet de la modification	Statut
20/07/2011	Création du document	Validé

Table des matières

1 Module 1 – Etude du contexte

Les risques évoqués dans ce document sont décrit dans le document de référence publié par l'ENISA (« Cloud computing : Benefits, risks and recommendations for information security », http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport) et dans celui publié par l'ANSSI « Externalisation des systèmes d'information ».

Un assureur s'attend à un pic de déclaration en cas d'évènements catastrophiques. Il fait appel à un service de type IAAS pour héberger et traiter les données de déclaration de sinistre. Ces données sont rapatriées dans son SI une fois instruites par les experts d'assurance.



1.1 Activité 1.1 – Définir le cadre de la gestion des risques

La définition détaillée du cadre de la gestion des risques sera faite avec le logiciel.

1.1.1 Identifier les sources de menaces

Types de sources de menaces	Retenu ou non	Exemple
Source humaine interne, malveillante, avec de faibles capacités	Oui	Employé malveillant Employé du prestataire malveillant
Source humaine interne, malveillante, avec des capacités importantes	Oui	
Source humaine interne, malveillante, avec des capacités illimitées	Oui	Administrateur malveillant Administrateur du prestataire malveillant
Source humaine externe, malveillante, avec de faibles capacités	Non	
Source humaine externe, malveillante, avec des capacités importantes	Oui	Pirate Concurrent
Source humaine externe, malveillante, avec des capacités illimitées	Non	
Source humaine interne, sans intention de nuire, avec de faibles capacités	Oui	Employé peu sérieux Employé du prestataire peu sérieux
Source humaine interne, sans intention de nuire, avec des capacités importantes	Oui	
Source humaine interne, sans intention de nuire, avec des capacités illimitées	Oui	Administrateur peu sérieux Administrateur du prestataire peu sérieux
Source humaine externe, sans intention de nuire, avec de faibles capacités	Non	
Source humaine externe, sans intention de nuire, avec des capacités importantes	Non	
Source humaine externe, sans intention de nuire, avec des capacités illimitées	Non	
Code malveillant d'origine inconnue	Non	
Phénomène naturel	Oui	Panne de matériel Panne de réseau
Catastrophe naturelle ou sanitaire	Oui	Inondation Tempête Tremblement de terre
Activité animale	Non	
Evènement interne	Oui	Faille dans l'application
Evènement externe	Oui	Décision du cloud provider Mauvaise gestion du prestataire Décision de justice Changement de juridiction

1.2 Activité 1.2 – Préparer les métriques

1.2.1 Activité 1.2.1 – Définir les critères de sécurité et élaborer les échelles de besoins

Afin d'exprimer les besoins de sécurité, les critères de sécurité retenus sont les suivants :

Critères de sécurité	Définitions
Disponibilité	Propriété d'accessibilité au moment voulu des biens essentiels
Intégrité	Propriété d'exactitude et de complétude des biens essentiels
Confidentialité	Propriété des biens essentiels de n'être accessibles que par utilisateurs autorisés

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de disponibilité :

Niveau de l'échelle	Description détaillée de l'échelle
Plus de 48h	Le bien essentiel peut être indisponible plus de 48 heures
Entre 24 et 48h	Le bien essentiel doit être disponible dans les 48 heures
Entre 4 et 24h	Le bien essentiel doit être disponible dans les 24 heures
Moins de 4h	Le bien essentiel doit être disponible dans les 4 heures

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes d'intégrité :

Niveau de l'échelle	Description détaillée de l'échelle
Détectable	Le bien essentiel peut ne pas être intègre si l'altération est identifiée
Maîtrisé	Le bien essentiel peut ne pas être intègre, si l'altération est identifiée et l'intégrité du bien essentiel retrouvée
Intègre	Le bien essentiel doit être rigoureusement intègre

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de confidentialité :

Niveau de l'échelle	Description détaillée de l'échelle
Public	Le bien essentiel est public
Limité	Le bien essentiel ne doit être accessible qu'au personnel et aux partenaires
Réservé	Le bien essentiel ne doit être accessible qu'au personnel interne impliqué
Privé	Le bien essentiel ne doit être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître

1.2.2 Activité 1.2.2 –Elaborer une échelle de niveaux de gravité

L'échelle suivante sera utilisée pour estimer la gravité des évènements redoutés et des risques.

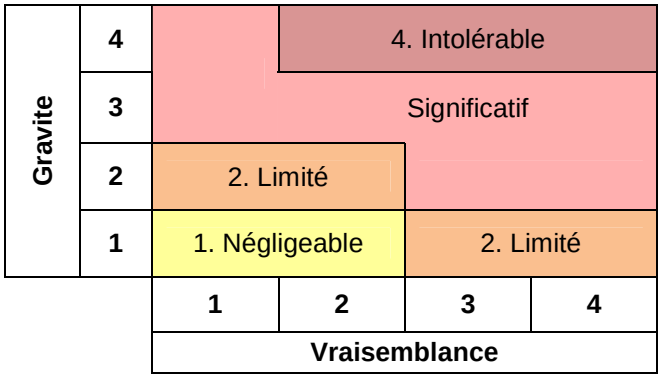
Niveau de l'échelle	Description détaillée de l'échelle
0. Insignifiant	L'évènement redouté n'est pas retenu dans le contexte de cette étude
1. Négligeable	La société surmontera les impacts sans aucune difficulté
2. Limitée	La société surmontera les impacts malgré quelques difficultés
3. Importante	La société surmontera les impacts avec de sérieuses difficultés
4. Critique	La société surmontera les impacts avec de très sérieuses difficultés et sur une très longue période

1.2.3 Activité 1.2.3 –Elaborer une échelle de niveaux de vraisemblance

L'échelle suivante sera utilisée pour estimer la vraisemblance des scénarios de menaces et des risques.

Niveau de l'échelle	Description détaillée de l'échelle
1. Minime	Cela ne devrait pas se (re)produire dans les 3 ans / Besoin des privilèges d'administrateur
2. Significative	Cela pourrait se (re)produire dans les 3 ans / Besoin de connaissances et d'un accès aux utilisateurs
3. Forte	Cela devrait se (re)produire dans l'année / Sans besoin de connaissances et avec un besoin d'accès aux utilisateurs
4. Maximale	Cela va certainement se (re)produire plusieurs fois dans l'année / Sans besoin de connaissances ni d'accès aux utilisateurs

1.2.4 Echelle de niveaux de risque



1.2.5 Critères de gestion des risques

Ce point sera à complété avec le logiciel.

1.3 Activité 1.3 – Identifier les biens

1.3.1 Biens essentiels

• Système d'information externalisé	• Données de déclaration de sinistre • Données de sécurité (Clés de chiffrement, logs, référentiel d'identité et des droits)
• Fonctions externalisées	• Traitement des données

1.3.2 Biens supports

• Système d'accès (SYS_AIN)	• Réseau de l'organisme • Réseau internet
• Système externalisé (SYS_EXT)	• Serveurs du prestataire • Postes de travail du prestataire • Logiciel d'administration du prestataire • Portail d'accès
• Système d'accès du prestataire (SYS_APR)	• Réseau du prestataire
• Organisation interne (ORG_INT)	• Utilisateurs (opérateurs en charge de la saisie, opérateurs en charge de l'instruction, auditeurs) • Administrateurs fonctionnels • Administrateurs techniques
• Organisation du prestataire (ORG_PRE)	• Administrateurs du cloud • Sous-traitants du Cloud Provider

1.3.3 Liens entre biens supports et biens essentiels

Biens essentiels / Biens supports	Données de déclaration de sinistre	Données de sécurité	Traitement des données
Système d'accès (SYS_AIN)	x	x	
Système externalisé (SYS_EXT)	x		x
Système d'accès du prestataire (SYS_APR)	x	x	
Organisation interne (ORG_INT)	x	x	
Organisation du prestataire (ORG_PRE)	x	x	

1.3.4 Mesures de sécurité existantes

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	9.1 Zones sécurisée	Périmètre de sécurité physique	Protéger les zones contenant des informations et des moyens de traitement de l'information par des périmètres de sécurité. Les serveurs doivent être inaccessibles par des personnes non autorisées et donc dans des salles hautement sécurisées.	x	x		Système du prestataire
2	9.1 Zones sécurisée	Contrôle physique des accès	Protéger les zones sécurisées pas des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité soit admis. Le prestataire doit donc surveiller et contrôler les accès aux datacenters et doit s'assurer que le personnel de maintenance ou de support ne peut menacer la sécurité des données, des matériels ou des logiciels.	X	x		Système du prestataire
3	9.1 Zones sécurisée	Protection contre les menaces extérieures et environnementales	Concevoir et appliquer des mesures de protection physiques contre les dommages causés par les incendies, les inondations, les tremblements de terre, les explosions, les troubles civils et autres formes de catastrophes naturelles ou de sinistre provoqués par l'homme. Les datacenters du prestataire devront satisfaire les exigences de sécurité liées à la protection physique des serveurs.	x	X		Système du prestataire
4	9.2 Sécurité du matériel	Services généraux	Protéger le matériel des coupures de courant et autres perturbations dues à une défaillance de services généraux.	x	x	x	Système du prestataire
5	9.2 Sécurité du matériel	Sécurité du câblage	Protéger les câbles électriques ou de télécommunications transportant des données contre toute interception ou dommage.		x		Système d'accès du prestataire
6	10.7 Manipulation des supports	Sécurité de la documentation système	La documentation décrivant l'ensemble du système doit être gardée avec un niveau de sécurité suffisant pour ne pas permettre à des personnes malveillantes d'avoir une connaissance poussée de l'architecture (mesures de « diffusion restreinte » systématiques).		x		Organisation interne / Organisation du prestataire
7	11.2 Gestion de l'accès utilisateur	Gestion des privilèges	Restreindre et contrôler l'attribution et l'utilisation des privilèges (gestion des habilitations).	x	x		Organisation interne
8	11.2 Gestion de l'accès utilisateur	Enregistrement des utilisateurs	Définir une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à accorder et à supprimer l'accès au cloud ou à son administration.	x	x		Organisation interne
9	11.2 Gestion de l'accès utilisateur	Gestion du mot de passe utilisateur	L'attribution de mots de passe doit être réalisée dans le cadre d'un processus formel.		x		Organisation interne / Système

							d'accès
10	11.3 Responsabilités utilisateurs	Utilisation du mot de passe	Demander aux utilisateurs de respecter les bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe.	x	x		Organisation interne / Système d'accès
11	11.4 Contrôle d'accès au réseau	Authentification des administrateurs	Afin d'accéder aux fonctions d'administration, les administrateurs doivent être authentifiés. L'authentification doit se faire de manière sécurisée (chiffrage des mots de passe, authentification à deux facteurs).		x		Système du prestataire
12	11.4 Contrôle d'accès au réseau	Authentification des utilisateurs	L'authentification des utilisateurs doit se faire de manière sécurisée par un cryptage des mots de passe et une authentification à deux facteurs.		x		Système du prestataire
13	14.1 Aspects de la sécurité de l'information en matière de gestion de l'activité	Plan de continuité de l'activité du prestataire	Le prestataire doit fournir les garanties de continuité de l'activité au travers d'un plan de continuité de l'activité. Ce PCA doit prendre en compte les exigences en matière de sécurité de l'information, les évènements pouvant être à l'origine d'interruption des processus métier, les mesures de restauration et de maintien de la disponibilité du système d'information, ainsi que la mise à l'essai dudit plan de continuité de l'activité.	x		x	Système du prestataire

2 Module 2 – Étude des évènements redoutés

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de déclaration de sinistre					
ER1	Divulgation des données	Privé	• Pirate • Employé du prestataire peu sérieux • Employé du prestataire malveillant • Bogue logiciel • Hébergeur/Faille dans l'application • Employé peu sérieux	• Perte de notoriété • Perte de confiance vis-à-vis des clients • Impossibilité de remplir des obligations légales • Action en justice à l'encontre de la société • Non-conformité aux labels de sécurité • Chute de valeur en bourse	4. Critique
ER2	Altération des données	Intègre	• Pirate • Employé du prestataire peu sérieux • Employé peu sérieux • Hébergeur/Faille dans l'application	• Impossibilité de remplir les obligations légales • Impossibilité d'assurer le traitement • Perte de confiance vis-à-vis des clients • Non-conformité aux labels de sécurité	3. Importante
ER3	Indisponibilité des données	24h	• Pirate • Employé du prestataire peu sérieux • Employé du prestataire malveillant • Hébergeur/Faille dans l'application • Entreprise tierce • Changement de juridiction • Panne de serveur • Bogue logiciel • Catastrophe naturelle	• Impossibilité d'assurer le traitement • Perte de confiance vis-à-vis des clients	2. Limitée
Données de sécurité					
ER4	Divulgation des données de sécurité	Privé	• Pirate	• Mise en péril du système d'information externalisé • Impossibilité de remplir les obligations légales • Non-conformité aux labels de sécurité • Perte de notoriété • Perte de confiance vis-à-vis des clients • Chute de valeur en bourse	4. Critique
ER5	Altération des données de sécurité	Intègre	• Pirate • Employé peu sérieux • Employé malveillant	• Perte de contrôle sur le système d'information externalisé • Impossibilité d'assurer le traitement	3. Importante
ER6	Indisponibilité des données de sécurité	48h	• Pirate • Employé malveillant	• Perte de contrôle sur le système d'information externalisé	2. Limitée
Traitement des données					
ER7	Divulgation de la fonction de traitement	Réservé	• Employé malveillant • Employé du prestataire malveillant • Pirate	• Perte d'un avantage concurrentiel	0. Insignifiant
ER8	Altération de la fonction de traitement	Intègre	• Employé malveillant • Employé du prestataire malveillant • Pirate	• Traitement des données non valide • Perte de confiance vis-à-vis des clients • Perte de notoriété • Perte de crédibilité	0. Insignifiant
ER9	Indisponibilité de la fonction de traitement	24h	• Mauvaise gestion du prestataire • Pirate • Concurrent • Employé malveillant • Panne de réseau	• Impossibilité d'assurer le traitement • Perte de confiance vis-à-vis des clients • Perte de notoriété	3. Importante

L'importance relative des évènements redoutés précédemment analysés est évaluée à l'aide du tableau suivant :

Gravité	Evénements redoutés
4. Critique	• ER1 Divulgation des données • ER4 Divulgation des données de sécurité
3. Importante	• ER2 Altération des données • ER5 Altération des données de sécurité • ER9 Indisponibilité de la fonction de traitement
2. Limitée	• ER3 Indisponibilité des données • ER6 Indisponibilité des données de sécurité
1. Négligeable	
0. Insignifiant	• ER7 Divulgation de la fonction de traitement • ER8 Altération de la fonction de traitement

3 Module 3 – Étude des scénarios de menaces

3.1 Système d'accès (SYS_AIN)

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système d'accès (SYS_AIN)	Menace sur le réseau internet causant une indisponibilité	D	• Entreprise tierce • Pirate • Concurrent • Employé malveillant • Panne de réseau	• M15 RSX-DEP Saturation du canal informatique • M16 RSX-DET Dégradation d'un canal informatique	• Blocage d'un lot d'adresses IP • Occupation de la bande passante (déni de service) • Rupture du canal d'accès au cloud	4. Maximale
	Menace sur le réseau internet causant une altération	I	• Pirate • Concurrent • Employé malveillant	• M13 RSX-USG Attaque du milieu sur un canal informatique	• Attaque de type Man in the Middle	3. Forte
	Menace sur le réseau internet causant une compromission	C	• Pirate • Concurrent • Employé malveillant	• M14 RSX-ESP Ecoute passive d'un canal informatique	• Acquisition de données par écoute passive	3. Forte

Menace	Vulnérabilités	Pré-requis	Vraisemblance
Blocage d'un lot d'adresses IP	• Possibilité d'être impliqué dans les activités frauduleuses d'une entreprise tierce sur le cloud	• Serveurs partagés (cloud public)	3. Forte
Occupation de la bande passante (déni de service)	• Réseau d'accès au cloud unique • Dimensionnement insuffisant de la bande passante	• Accès à la table de routage • Accès aux utilisateurs	2. Significative
Rupture du canal d'accès au cloud	• Réseau d'accès au cloud unique • Dimensionnement insuffisant de la bande passante	• Contrôle insuffisant du matériel • Accès physique au réseau	4. Maximale
Acquisition de données par écoute passive	• Réseau perméable • Données transmises interprétables	• Accès à la table de routage • Accès aux utilisateurs	3. Forte
Attaque de type Man in the Middle	• Possibilité de falsification du service appelé • Routage altérable	• Accès à la table de routage • Accès aux utilisateurs	3. Forte

Mesures de sécurité existantes

N°	Thème ISO 27002	Mesures de sécurité existantes	Description	Prévention	Protection	Récupération	Bien support
9	11.2 Gestion de l'accès utilisateur	Gestion du mot de passe utilisateur	L'attribution de mots de passe doit être réalisée dans le cadre d'un processus formel.		x		Organisation interne / Système d'accès
10	11.3 Responsabilités utilisateurs	Utilisation du mot de passe	Demander aux utilisateurs de respecter les bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe.	x	x		Organisation interne / Système d'accès

Mesures de sécurité complémentaires

N°	Thème ISO 27002	Mesures de sécurité	Description	Prévention	Protection	Récupération	Bien support
9	10.3 Planification et acceptation du système	Dimensionnement	Les ressources doivent correspondre aux besoins. Il est nécessaire de faire des projections et des tests de performance pour connaître les limites du système et pouvoir anticiper toute surcharge. Ainsi, le prestataire doit s'assurer que les ressources allouées aux différents utilisateurs du service sont suffisantes pour couvrir les besoins.	x			Système d'accès / Système du prestataire / Système d'accès du prestataire
11	10.10 Surveillance	Protection des informations journalisées	Protection des équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés. Analyser les journaux à l'aide d'un logiciel de contrôle de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte.	x	x		Système d'accès / Système du prestataire / Système

							d'accès du prestataire
12	10.10 Surveillance	Journal administrateur et journal des opérations	La journalisation des opérations des administrateurs permet de garder une trace des actions des administrateurs.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
13	10.10 Surveillance	Rapports de défaut	Journaliser et analyser les éventuels défauts et prendre les mesures appropriées.		x	x	Système d'accès / Système du prestataire / Système d'accès du prestataire
14	10.10 Surveillance	Audit de la passerelle d'accès au cloud	La passerelle d'accès au cloud doit être soumise à un audit régulier (annuel) pour vérifier que les mesures de sécurité sont effectives et en adéquation avec les objectifs de sécurité.	x			Système d'accès
17	11.4 Contrôle d'accès au réseau	Contrôle du routage réseau interne	S'assurer que l'organisation mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		Système d'accès
20	12.3 Mesures cryptographiques	Chiffrement des flux	Les flux contenant des informations sensibles ou à caractère personnel doivent être chiffrées.	x			Système d'accès
21	12.3 Mesures cryptographiques	Gestion des clés	Une procédure de gestion des clés doit venir à l'appui de la politique de l'organisme en matière de chiffrement.	x			Système du prestataire / Système d'accès

3.2 Système du prestataire (SYS_EXT)

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système du prestataire (SYS_EXT)	Menace sur le système du prestataire causant une indisponibilité	D	• Employé du prestataire peu sérieux • Employé du prestataire malveillant • Décision du cloud provider • Concurrent • Pirate • Hébergeur/Faille dans l'application • Décision de justice • Panne de matériel • Bogue logiciel • Catastrophe naturelle	• M9 LOG-DEP Dépassement des limites d'un logiciel • M12 LOG-PTE Disparition d'un logiciel • M6 MAT-PTE Perte d'un matériel • M7 LOG-USG Détournement de l'usage prévu d'un logiciel • M4 MAT-PTE Détérioration d'un matériel • M11 LOG-MOD Modification d'un logiciel	• Surexploitation du système du prestataire • Cessation d'activité du prestataire • Serveurs du prestataire saisis par la justice • Perte ou effacement des données • Changement des données du portail d'accès au cloud	3. Forte
	Menace sur le système du prestataire causant une altération	I	• Employé du prestataire peu sérieux • Employé du prestataire malveillant • Pirate • Hébergeur/Faille dans l'application	• M7 LOG-USG Détournement de l'usage prévu d'un logiciel • M11 LOG-MOD Modification d'un logiciel	• Données rendues accessibles à d'autres utilisateurs du cloud	3. Forte
	Menace sur le système du prestataire causant une compromission	C	• Décision du cloud provider • Pirate • Concurrent • Employé peu sérieux • Employé du prestataire peu sérieux • Employé du prestataire malveillant • Hébergeur/Faille dans l'application • Bogue logiciel • Panne de matériel • Décision de justice	• M8 LOG-ESP Analyse d'un logiciel • M6 MAT-PTE Perte d'un matériel • M7 LOG-USG Détournement de l'usage prévu d'un logiciel	• Collecte de données d'accès au SI externalisé • Prestataire racheté par une société investissant moins dans la sécurité • Serveurs du prestataire saisis par la justice • Vol de serveurs • Données non effacées des serveurs du prestataire et rendues accessibles • Données rendues accessibles à d'autres utilisateurs du cloud • Changement des données du portail d'accès au cloud	4. Maximale

Menace	Vulnérabilités	Pré-requis	Vraisemblance
Surexploitation du système du prestataire	• Manque de compétence du personnel du prestataire • Négligence du personnel du prestataire	• Ressources allouées par le prestataire insuffisantes	1. Minime
Cessation d'activité du prestataire	• Portabilité des données non assurée	• Fébrilité économique du prestataire	2. Significative
Serveurs du prestataire saisis par la justice	• Juridiction liée à la position géographique des données	• Changement de juridiction dans le pays où sont situés les serveurs Ou • Une entreprise tierce mène des activités frauduleuses sur le cloud Ou • Juridiction relative au stockage des données personnelles	2. Significative
Perte ou effacement des données	• Données accessibles avec les droits adéquats • Matériel peu fiable • Matériel inapproprié aux conditions d'utilisation • Datacenter mal protégé contre les catastrophes naturelles • Mauvaise compartimentation du logiciel	• Privilèges élevés sur l'application Ou • Contrôle insuffisant du matériel Ou • Bogue dans le logiciel utilisé Ou • Datacenter dans une zone à risque de catastrophes naturelles Ou • Serveurs partagés (cloud public)	3. Forte

Collecte de données d'accès au SI externalisé	• SI du sous-traitant mal sécurisé • Faille dans l'application	• Accès physique ou logique au SI du sous-traitant • Connaissance de l'existence du logiciel • Connaissance de l'existence du portail d'accès	4. Maximale
Changement des données du portail d'accès au cloud	• Faille dans le portail d'accès au cloud • Négligence du personnel du prestataire	• Accès physique ou logique au portail d'accès • Connaissance de l'existence du portail d'accès	3. Forte
Prestataire racheté par une société investissant moins dans la sécurité	• Manque de compétence du personnel du prestataire • Négligence du personnel du prestataire	• Fébrilité économique du prestataire	2. Significative
Données non effacées des serveurs du prestataire et rendues accessibles	• Mauvais effacement des données par le prestataire	• Serveurs partagés ou réutilisés	3. Forte
Données rendues accessibles à d'autres utilisateurs du cloud	• Mauvaise compartimentation du logiciel	• Serveurs partagés ou réutilisés	3. Forte
Vol de serveurs	• Manque de sécurisation des datacenters • Négligence du personnel du prestataire • Négligence du personnel de sécurité du datacenter	• Accès physique aux serveurs • Connaissance de l'existence et de la localisation des serveurs • Possibilité de déplacer un serveur	3. Forte

Mesures de sécurité existantes

N°	Thème ISO 27002	Mesures de sécurité existantes	Description	Prévention	Protection	Récupération	Bien support
1	9.1 Zones sécurisée	Périmètre de sécurité physique	Protéger les zones contenant des informations et des moyens de traitement de l'information par des périmètres de sécurité. Les serveurs doivent être inaccessibles par des personnes non autorisées et donc dans des salles hautement sécurisées.	x	x		Système du prestataire
2	9.1 Zones sécurisée	Contrôle physique des accès	Protéger les zones sécurisées pas des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité soit admis. Le prestataire doit donc surveiller et contrôler les accès aux datacenters et doit s'assurer que le personnel de maintenance ou de support ne peut menacer la sécurité des données, des matériels ou des logiciels.	X	x		Système du prestataire
3	9.1 Zones sécurisée	Protection contre les menaces extérieures et environnementales	Concevoir et appliquer des mesures de protection physiques contre les dommages causés par les incendies, les inondations, les tremblements de terre, les explosions, les troubles civils et autres formes de catastrophes naturelles ou de sinistre provoqués par l'homme. Les datacenters du prestataire devront satisfaire les exigences de sécurité liées à la protection physique des serveurs.	x	X		Système du prestataire
4	9.2 Sécurité du matériel	Services généraux	Protéger le matériel des coupures de courant et autres perturbations dues à une défaillance de services généraux.	x	x	x	Système du prestataire
11	11.4 Contrôle d'accès au réseau	Authentification des administrateurs	Afin d'accéder aux fonctions d'administration, les administrateurs doivent être authentifiés. L'authentification doit se faire de manière sécurisée (chiffrage des mots de passe, authentification à deux facteurs).		x		Système du prestataire
12	11.4 Contrôle d'accès au réseau	Authentification des utilisateurs	L'authentification des utilisateurs doit se faire de manière sécurisée par un cryptage des mots de passe et une authentification à deux facteurs.		x		Système du prestataire
13	14.1 Aspects de la sécurité de l'information en matière de gestion de l'activité	Plan de continuité de l'activité du prestataire	Le prestataire doit fournir les garanties de continuité de l'activité au travers d'un plan de continuité de l'activité. Ce PCA doit prendre en compte les exigences en matière de sécurité de l'information, les évènements pouvant être à l'origine d'interruption des processus métier, les mesures de restauration et de maintien de la disponibilité du système d'information, ainsi que la mise à l'essai dudit plan de continuité de l'activité.	x		x	Système du prestataire

Mesures de sécurité complémentaires

N°	Thème ISO 27002	Mesures de sécurité	Description	Prévention	Protection	Récupération	Bien support
5	9.2 Sécurité du matériel	Mise au rebut ou recyclage sécurisé du matériel	Vérifier tout le matériel contenant des supports de stockage pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut. Le prestataire devra préciser les mesures mises en œuvre pour assurer la mise au rebut de ses matériels.	x	x		Système du prestataire
6	10.2 Gestion de la prestation de service par un tiers	Prestation de service et contrat	S'assurer que les mesures de sécurité, les définitions du service et les niveaux de prestation prévus dans l'accord de prestation de service tiers sont mis en œuvre, appliqués et tenus à jour par le tiers. Notamment, le contrat de prestation de service doit inclure les éléments liés à la journalisation d'évènements, au suivi du service hébergé (mise à jour, maintenances, sauvegardes…), aux modalités de prévention d'une attaque et à la réaction suite à un incident.				Système du prestataire

7	10.2 Gestion de la prestation de service par un tiers	Clause contractuelle de restitution des données	Le contrat de prestation de service doit préciser les conditions de restitution des données (conditions, délais, formats) pour permettre le rapatriement des données ou le changement de prestataire sans interruption de service.	x		x	Système du prestataire
8	10.2 Gestion de la prestation de service par un tiers	Gestion des modifications dans les services tiers	Gérer les changements effectués dans la prestation de service, comprenant le maintien et l'amélioration des politiques, procédures et mesures existantes. Notamment, le contrat doit permettre la validation des choix du prestataire lors de la mise en œuvre de nouvelles solutions logicielles ou matérielles (pour éviter la perte de sécurité).	x	x		Système du prestataire
9	10.3 Planification et acceptation du système	Dimensionnement	Les ressources doivent correspondre aux besoins. Il est nécessaire de faire des projections et des tests de performance pour connaître les limites du système et pouvoir anticiper toute surcharge. Ainsi, le prestataire doit s'assurer que les ressources allouées aux différents utilisateurs du service sont suffisantes pour couvrir les besoins.	x			Système d'accès / Système du prestataire / Système d'accès du prestataire
10	10.5 Sauvegarde	Sauvegarde des informations - backups	Le prestataire doit prendre toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé. Il doit notamment effectuer un double exemplaire des sauvegardes et doit les conserver dans des locaux physiquement séparés.	x	x	x	Système du prestataire
11	10.10 Surveillance	Protection des informations journalisées	Protection des équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés. Analyser les journaux à l'aide d'un logiciel de contrôle de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
12	10.10 Surveillance	Journal administrateur et journal des opérations	La journalisation des opérations des administrateurs permet de garder une trace des actions des administrateurs.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
13	10.10 Surveillance	Rapports de défaut	Journaliser et analyser les éventuels défauts et prendre les mesures appropriées.		x	x	Système d'accès / Système du prestataire / Système d'accès du prestataire
15	11.4 Contrôle d'accès au réseau	Protection des ports de diagnostic et de configuration à distance	Le prestataire doit contrôler l'accès physique et logique aux ports de diagnostic et de configuration à distance.	x	x		Système du prestataire / Système d'accès du prestataire
19	12.3 Mesures cryptographiques	Politique d'utilisation des mesures cryptographiques	Elaboration et mise en œuvre d'une politique d'utilisation des mesures cryptographiques en vue de protéger l'information. Par exemple, employer un logiciel de chiffrement des données externalisées.	x			Système du prestataire
21	12.3 Mesures cryptographiques	Gestion des clés	Une procédure de gestion des clés doit venir à l'appui de la politique de l'organisme en matière de chiffrement.	x			Système du prestataire / Système d'accès
22	12.6 Gestion des vulnérabilités techniques	Mesures relatives aux vulnérabilités techniques	Le prestataire doit tenir informé l'organisation (assureur) en temps voulu de toute vulnérabilité technique des systèmes d'information en exploitation, évaluer l'exposition de l'organisation auxdites vulnérabilités et entreprendre les actions appropriées pour traiter le risque associé. Cette démarche doit être formalisée dans le contrat de service.	x			Système du prestataire
23	15.1 Conformité avec les exigences légales	Protection des données et confidentialité des informations relatives à la vie privée	Le prestataire doit satisfaire les exigences de protection et de confidentialité des données à caractère personnel telles que l'exigent la législation ou les réglementations applicables. Le transfert des données à caractère personnel en dehors des frontières de l'Union européenne est réglementé par la directive européenne 95/46/CE et la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.		x		Système du prestataire
24		Hébergement non mutualisé	L'hébergement doit être réalisé sur une ou plusieurs machines spécifiques (non mutualisé). Ainsi, les données de l'organisation (assureur) ne risquent pas de subir les conséquences d'une activité frauduleuse d'un autre client du cloud. Les problèmes de compartimentation sont de plus écartés.	x			Système du prestataire
25	15.1 Conformité avec les exigences légales	Localisation des données	Le prestataire doit être en mesure d'indiquer la localisation des données pour informer l'organisation	x			Système du prestataire

3.3 Système d'accès du prestataire (SYS_APR)

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système d'accès du prestataire (SYS_APR)	Menace sur le réseau du prestataire causant une indisponibilité	D	• Pirate • Employé du prestataire malveillant • Panne de réseau	• M15 RSX-DEP Saturation du canal informatique • M16 RSX-DET Dégradation d'un canal informatique	• Perte de liaison entre les serveurs du prestataire	3. Forte
	Menace sur le réseau du prestataire causant une altération	I	• Pirate • Employé du prestataire malveillant	• M13 RSX-USG Attaque du milieu sur un canal informatique • M11 LOG-MOD Modification d'un logiciel	• Attaque de type Man in the Middle • Changement des données du portail d'accès au cloud	3. Forte
	Menace sur le réseau du prestataire causant une compromission	C	• Pirate • Employé du prestataire malveillant	• M14 RSX-ESP Ecoute passive d'un canal informatique	• Acquisition de données par écoute passive entre les serveurs du prestataire	3. Forte

Menace	Vulnérabilités	Pré-requis	Vraisemblance
Perte de liaison entre les serveurs du prestataire	• Réseau d'accès au cloud unique • Dimensionnement insuffisant de la bande passante	• Accès à la table de routage • Accès aux utilisateurs	3. Forte
Attaque de type Man in the Middle	• Possibilité de falsification du service appelé • Routage altérable	• Accès à la table de routage • Accès aux utilisateurs	3. Forte
Acquisition de données par écoute passive entre les serveurs du prestataire	• Perméabilité du réseau • Données observables lors du transfert	• Accès à la table de routage • Accès aux utilisateurs	3. Forte
Changement des données du portail d'accès au cloud	• Données du portail d'accès modifiables • Données du portail d'accès accessibles avec les droits adéquats	• Accès physique ou logique au portail d'accès • Connaissance de l'existence du portail d'accès	3. Forte

Mesures de sécurité existantes

N°	Thème ISO 27002	Mesures de sécurité existantes	Description	Prévention	Protection	Récupération	Bien support
5	9.2 Sécurité du matériel	Sécurité du câblage	Protéger les câbles électriques ou de télécommunications transportant des données contre toute interception ou dommage.		x		Système d'accès du prestataire

Mesures de sécurité complémentaires

N°	Thème ISO 27002	Mesures de sécurité	Description	Prévention	Protection	Récupération	Bien support
9	10.3 Planification et acceptation du système	Dimensionnement	Les ressources doivent correspondre aux besoins. Il est nécessaire de faire des projections et des tests de performance pour connaître les limites du système et pouvoir anticiper toute surcharge. Ainsi, le prestataire doit s'assurer que les ressources allouées aux différents utilisateurs du service sont suffisantes pour couvrir les besoins.	x			Système d'accès / Système du prestataire / Système d'accès du prestataire
11	10.10 Surveillance	Protection des informations journalisées	Protection des équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés. Analyser les journaux à l'aide d'un logiciel de contrôle de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
12	10.10 Surveillance	Journal administrateur et journal des opérations	La journalisation des opérations des administrateurs permet de garder une trace des actions des administrateurs.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire

13	10.10 Surveillance	Rapports de défaut	Journaliser et analyser les éventuels défauts et prendre les mesures appropriées.		x	x	Système d'accès / Système du prestataire / Système d'accès du prestataire
15	11.4 Contrôle d'accès au réseau	Protection des ports de diagnostic et de configuration à distance	Le prestataire doit contrôler l'accès physique et logique aux ports de diagnostic et de configuration à distance.	x	x		Système du prestataire / Système d'accès du prestataire
16	11.4 Contrôle d'accès au réseau	Mesure relative à la connexion réseau	Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme du prestataire, il convient de vérifier que le prestataire restreigne la capacité de connexion réseau des utilisateurs, conformément à la politique de contrôle d'accès et les exigences relatives aux applications de gestion.	x	x		Système d'accès du prestataire
18	11.4 Contrôle d'accès au réseau	Contrôle du routage réseau du prestataire	S'assurer que le prestataire mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		Système d'accès du prestataire

3.4 Organisation interne (ORG_INT)

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Organisation interne (ORG_INT)	Menace sur l'organisation interne causant une indisponibilité	D	• Employé peu sérieux • Pirate	• M23 PER-MOD Influence sur une personne	• Collecte de données d'accès au SI externalisé • Suppression des données par le personnel sous influence d'un pirate	2. Significative
	Menace sur l'organisation interne causant une altération	I	• Employé peu sérieux	• M21 PER-DEP Surcharge des capacités d'une personne	• Mauvaise répartition des rôles entre le personnel interne et le personnel du prestataire	1. Minime
	Menace sur l'organisation interne causant une compromission	C	• Employé malveillant	• M23 PER-MOD Influence sur une personne	• L'employé se venge	3. Forte

Menace	Vulnérabilités	Pré-requis	Vraisemblance
Mauvaise répartition des rôles entre le personnel interne et le personnel du prestataire	• Manque de compétence du personnel • Négligence du personnel	• Partage de l'administration entre le personnel interne et le personnel du prestataire	1. Minime
Collecte de données d'accès au SI externalisé	• Personne influençable ou manipulable	• Etablissement d'une relation avec la personne	2. Significative
Suppression des données par le personnel sous influence d'un pirate	• Personne influençable ou manipulable	• Etablissement d'une relation avec la personne	2. Significative
L'employé se venge	• Personne influençable ou manipulable	• Privilèges élevés sur l'application • Motivation de la vengeance	3. Forte

Mesures de sécurité existantes

N°	Thème ISO 27002	Mesures de sécurité existantes	Description	Prévention	Protection	Récupération	Bien support
6	10.7 Manipulation des supports	Sécurité de la documentation système	La documentation décrivant l'ensemble du système doit être gardée avec un niveau de sécurité suffisant pour ne pas permettre à des personnes malveillantes d'avoir une connaissance poussée de l'architecture (mesures de « diffusion restreinte » systématiques).		x		Organisation interne / Organisation du prestataire
7	11.2 Gestion de l'accès utilisateur	Gestion des privilèges	Restreindre et contrôler l'attribution et l'utilisation des privilèges (gestion des habilitations).	x	x		Organisation interne
8	11.2 Gestion de l'accès utilisateur	Enregistrement des utilisateurs	Définir une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à accorder et à supprimer l'accès au cloud ou à son administration.	x	x		Organisation interne
9	11.2 Gestion de l'accès utilisateur	Gestion du mot de passe utilisateur	L'attribution de mots de passe doit être réalisée dans le cadre d'un processus formel.		x		Organisation interne / Système d'accès
10	11.3 Responsabilités utilisateurs	Utilisation du mot de passe	Demander aux utilisateurs de respecter les bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe.	x	x		Organisation interne / Système d'accès

Mesures de sécurité complémentaires

N°	Thème ISO 27002	Mesures de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	6.1 Organisation interne	Attribution des responsabilités en matière de sécurité de l'information	Il convient de définir clairement toutes les responsabilités en matière de sécurité de l'information. La répartition des responsabilités entre le personnel interne et le personnel du prestataire doit être formalisée et respectée.	x			Organisation interne / Organisation externe

2	8.2 Pendant la durée du contrat	Sensibilisation, qualification et formations en matière de sécurité de l'information	Le personnel interne doit être formé aux bonnes pratiques de sécurité. Il doit avoir un niveau de sensibilisation pertinent pour ses fonctions. Cela passe par des sessions de formation et des missives d'information concernant la sécurité.	x	x		Organisation interne
3	8.2 Pendant la durée du contrat	Procédures disciplinaires	Mettre en place un processus disciplinaire clair pour toute ayant enfreint les règles de sécurité pour réduire les risques d'influence et de corruption. Par exemple, les sanctions peuvent être précisées dans une charte définissant les engagements de responsabilités.	x	x		Organisation interne
4	8.3 Fin ou modification de contrat	Retrait des droits d'accès	Les droits d'accès de tout utilisateur ou administrateur aux données et aux logiciels doivent être supprimés en fin de contrat ou doivent être modifiés en cas de changement de contrat ou de responsabilités.	x			Organisation interne

3.5 Organisation du prestataire (ORG_PRE)

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Organisation du prestataire (ORG_PRE)	Menace sur l'organisation du prestataire causant une indisponibilité	D	• Employé du prestataire peu sérieux • Pirate	• M23 PER-MOD Influence sur une personne	• Collecte de données d'accès au SI externalisé • Suppression des données par le personnel sous influence d'un pirate	2. Significative
	Menace sur l'organisation du prestataire causant une altération	I	• Employé peu sérieux	• M21 PER-DEP Surcharge des capacités d'une personne	• Mauvaise répartition des rôles entre le personnel interne et le personnel du prestataire	1. Minime
	Menace sur l'organisation du prestataire causant une compromission	C	• Employé malveillant	• M23 PER-MOD Influence sur une personne	• L'employé se venge	3. Forte

Menace	Vulnérabilités	Pré-requis	Vraisemblance
Mauvaise répartition des rôles entre le personnel interne et le personnel du prestataire	• Manque de compétence du personnel • Négligence du personnel	• Partage de l'administration entre le personnel interne et le personnel du prestataire	1. Minime
Collecte de données d'accès au SI externalisé	• Personne influençable ou manipulable	• Etablissement d'une relation avec la personne	2. Significative
Suppression des données par le personnel sous influence d'un pirate	• Personne influençable ou manipulable	• Etablissement d'une relation avec la personne	2. Significative
L'employé se venge	• Personne influençable ou manipulable	• Privilèges élevés sur l'application • Motivation de la vengeance	3. Forte

Mesures de sécurité existantes

N°	Thème ISO 27002	Mesures de sécurité existantes	Description	Prévention	Protection	Récupération	Bien support
6	10.7 Manipulation des supports	Sécurité de la documentation système	La documentation décrivant l'ensemble du système doit être gardée avec un niveau de sécurité suffisant pour ne pas permettre à des personnes malveillantes d'avoir une connaissance poussée de l'architecture (mesures de « diffusion restreinte » systématiques).		x		Organisation interne / Organisation du prestataire

Mesures de sécurité complémentaires

N°	Thème ISO 27002	Mesures de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	6.1 Organisation interne	Attribution des responsabilités en matière de sécurité de l'information	Il convient de définir clairement toutes les responsabilités en matière de sécurité de l'information. La répartition des responsabilités entre le personnel interne et le personnel du prestataire doit être formalisée et respectée.	x			Organisation interne / Organisation externe

L'importance relative des scénarios de menaces précédemment analysés est évaluée de la façon suivante :

Vraisemblance	Scénarios de menaces
4. Maximale	• Menace sur le réseau internet causant une indisponibilité • Menace sur le système du prestataire causant une compromission
3. Forte	• Menace sur le réseau internet causant une altération • Menace sur le réseau internet causant une compromission • Menace sur le système du prestataire causant une indisponibilité • Menace sur le système du prestataire causant une altération • Menace sur le réseau du prestataire causant une indisponibilité • Menace sur le réseau du prestataire causant une altération • Menace sur le réseau du prestataire causant une compromission • Menace sur l'organisation interne causant une compromission • Menace sur l'organisation du prestataire causant une compromission
2. Significative	• Menace sur l'organisation interne causant une indisponibilité • Menace sur l'organisation du prestataire causant une indisponibilité
1. Minime	• Menace sur l'organisation interne causant une altération • Menace sur l'organisation du prestataire causant une altération

4 Module 4 – Étude des risques

4.1 Analyse et évaluation des risques

4.1.1 Divulgation des données de déclaration de sinistre

Scénarios décrits dans les documents (ANSSI et ENISA)

Bien(s) support(s)	Scénario(s) de menace
Système du prestataire – Logiciel d'administration du prestataire	Le Cloud Provider fait appel à un prestataire offrant de plus faibles garanties de sécurité : un pirate accède aux données via le SI de ce prestataire.
Système du prestataire – Logiciel d'administration du prestataire	Le Cloud Provider est racheté par une société investissant moins dans la sécurité : une faille permet à un pirate de s'introduire dans le système.
Système du prestataire – Serveurs du prestataire	Les données confidentielles et soumises à des réglementations sont stockées à l'étranger. La réglementation du pays où sont stockées les données permet une divulgation de ces données. Les données peuvent être saisies par la justice.
Système du prestataire – Logiciel d'administration du prestataire	Les données confidentielles soumises à des réglementations sont stockées dans le cloud. Cette externalisation rend possible l'accès aux données par un pirate.
Système du prestataire – Logiciel d'administration du prestataire	L'administrateur du cloud n'efface délibérément pas les données stockées sur les serveurs.
Système du prestataire – Logiciel d'administration du prestataire	L'administrateur du cloud oublie d'effacer tout ou partie des données stockées sur le serveur.
Système du prestataire – Logiciel d'administration du prestataire	Un bogue logiciel laisse des traces de données sur les serveurs.
Système du prestataire – Logiciel d'administration du prestataire	Les données de plusieurs sociétés sont stockées sur un même support : leur mauvaise séparation entraîne une divulgation non-intentionnelle des données.
Système du prestataire – Logiciel d'administration du prestataire	Le piratage des droits d'un administrateur du cloud permet l'accès à tout le système.
Personnel interne ou personnel du prestataire	Un pirate utilise les techniques de « social engineering » pour obtenir l'accès aux données.
Personnel du prestataire	Un employé du prestataire souhaitant se venger divulgue des données.
Système d'accès – Internet	Un pirate intercepte sur Internet les données transitant entre le système interne et le cloud.
Système d'accès du prestataire – Réseau du prestataire	Un pirate ou un employé du Cloud Provider intercepte les données transitant entre les serveurs du cloud.
Système du prestataire - Serveurs du prestataire	Un pirate ou un employé du Cloud Provider obtient de manière frauduleuse l'accès aux serveurs de données
Système du prestataire - Serveurs du prestataire	Un pirate ou un employé du Cloud Provider dérobe les serveurs de backup des données

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de déclaration de sinistre					
ER1	Divulgation des données	Privé	• Pirate • Employé du prestataire peu sérieux • Employé du prestataire malveillant • Bogue logiciel • Hébergeur/Faille dans l'application • Employé peu sérieux	• Perte de notoriété • Perte de confiance vis-à-vis des clients • Impossibilité de remplir des obligations légales • Action en justice à l'encontre de la société • Non-conformité aux labels de sécurité • Chute de valeur en bourse	4. Critique

Résultat obtenu par le logiciel

Bien support	Scénarios de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance

Système d'accès (SYS_AIN)	Menace sur le réseau internet causant une compromission	C	• Pirate • Concurrent • Employé malveillant	• M14 RSX-ESP Ecoute passive d'un canal informatique	• Acquisition de données par écoute passive	3. Forte
Système du prestataire (SYS_EXT)	Menace sur le système du prestataire causant une compromission	C	• Décision du cloud provider • Pirate • Employé peu sérieux • Employé du prestataire peu sérieux • Employé du prestataire malveillant • Hébergeur/Faille dans l'application • Bogue logiciel • Panne de matériel • Décision de justice	• M8 LOG-ESP Analyse d'un logiciel • M6 MAT-PTE Perte d'un matériel • M7 LOG-USG Détournement de l'usage prévu d'un logiciel	• Collecte de données d'accès au SI externalisé • Prestataire racheté par une société investissant moins dans la sécurité • Serveurs du prestataire saisis par la justice • Accès physique aux serveurs • Vol de serveur • Données non effacées des serveurs du prestataire et rendues accessibles • Données rendues accessibles à d'autres utilisateurs du cloud • Changement des données du portail d'accès au cloud	4. Maximale
Système d'accès du prestataire (SYS_APR)	Menace sur le réseau du prestataire causant une compromission	C	• Pirate • Employé du prestataire malveillant	• M14 RSX-ESP Ecoute passive d'un canal informatique	• Acquisition de données par écoute passive entre les serveurs du prestataire	3. Forte
Organisation interne (ORG_INT)	Menace sur l'organisation interne causant une compromission	C	• Employé malveillant	• M23 PER-MOD Influence sur une personne	• L'employé se venge	3. Forte
Organisation du prestataire (ORG_PRE)	Menace sur l'organisation du prestataire causant une compromission	C	• Employé malveillant	• M23 PER-MOD Influence sur une personne	• L'employé se venge	3. Forte

Menace	Vulnérabilités	Pré-requis	Vraisemblance
Acquisition de données par écoute passive	• Réseau perméable • Données transmises interprétables	• Accès à la table de routage • Accès aux utilisateurs	3. Forte
Serveurs du prestataire saisis par la justice	• Juridiction liée à la position géographique des données	• Changement de juridiction dans le pays où sont situés les serveurs Ou • Une entreprise tierce mène des activités frauduleuses sur le cloud Ou • Juridiction relative au stockage des données personnelles	2. Significative
Données rendues accessibles à d'autres utilisateurs du cloud	• Mauvaise compartimentation du logiciel	• Serveurs partagés (cloud public) ou réutilisés	2. Significative
Collecte de données d'accès au SI externalisé	• SI du sous-traitant mal sécurisé • Faille dans l'application	• Accès physique ou logique au SI du sous-traitant • Connaissance de l'existence du logiciel • Connaissance de l'existence du portail d'accès	4. Maximale
Changement des données du portail d'accès au cloud	• Faille dans le portail d'accès au cloud • Négligence du personnel du prestataire	• Accès physique ou logique au portail d'accès • Connaissance de l'existence du portail d'accès	3. Forte
Prestataire racheté par une société investissant moins dans la sécurité	• Manque de compétence du personnel du prestataire • Négligence du personnel du prestataire	• Fébrilité économique du prestataire	2. Significative
Données non effacées des serveurs du prestataire et rendues accessibles	• Mauvais effacement des données par le prestataire	• Serveurs partagés ou réutilisés	3. Forte
Accès physique aux serveurs	• Manque de sécurisation des datacenters • Négligence du personnel du prestataire	• Accès physique aux serveurs • Connaissance de l'existence et de la localisation des serveurs	3. Forte
Vol de serveurs	• Manque de sécurisation des datacenters • Négligence du personnel du prestataire • Négligence du personnel de sécurité du datacenter	• Accès physique aux serveurs • Connaissance de l'existence et de la localisation des serveurs • Possibilité de déplacer un serveur	3. Forte
Acquisition de données par écoute passive entre les serveurs du prestataire	• Perméabilité du réseau • Données observables lors du transfert	• Accès à la table de routage • Accès aux utilisateurs	3. Forte
L'employé se venge	• Personne influençable ou manipulable	• Privilèges élevés sur l'application • Motivation de la vengeance	3. Forte

Niveau de risque avant application des mesures

Niveau de risque	1. Négligeable	2. Limité	3. Significatif	**4. Intolérable**
Gravité	1. Négligeable	2. Limitée	3. Importante	**4. Critique**
Vraisemblance	1. Minime	2. Significative	3. Forte	**4. Maximale**

Mesures de sécurité existantes

N°	Thème ISO 27002	Mesures de sécurité existantes	Description	Prévention	Protection	Récupération	Bien support
1	9.1 Zones sécurisée	Périmètre de sécurité physique	Protéger les zones contenant des informations et des moyens de traitement de l'information par des périmètres de sécurité. Les serveurs doivent être inaccessibles par des personnes non autorisées et donc dans des salles hautement sécurisées.	x	x		Système du prestataire
2	9.1 Zones sécurisée	Contrôle physique des accès	Protéger les zones sécurisées pas des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité soit admis. Le prestataire doit donc surveiller et contrôler les accès aux datacenters et doit s'assurer que le personnel de maintenance ou de support ne peut menacer la sécurité des données, des matériels ou des logiciels.	X	x		Système du prestataire
5	9.2 Sécurité du matériel	Sécurité du câblage	Protéger les câbles électriques ou de télécommunications transportant des données contre toute interception ou dommage.		x		Système d'accès du prestataire
6	10.7 Manipulation des supports	Sécurité de la documentation système	La documentation décrivant l'ensemble du système doit être gardée avec un niveau de sécurité suffisant pour ne pas permettre à des personnes malveillantes d'avoir une connaissance poussée de l'architecture (mesures de « diffusion restreinte » systématiques).		x		Organisation interne / Organisation du prestataire
7	11.2 Gestion de l'accès utilisateur	Gestion des privilèges	Restreindre et contrôler l'attribution et l'utilisation des privilèges (gestion des habilitations).	x	x		Organisation interne
8	11.2 Gestion de l'accès utilisateur	Enregistrement des utilisateurs	Définir une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à accorder et à supprimer l'accès au cloud ou à son administration.	x	x		Organisation interne
9	11.2 Gestion de l'accès utilisateur	Gestion du mot de passe utilisateur	L'attribution de mots de passe doit être réalisée dans le cadre d'un processus formel.		x		Organisation interne / Système d'accès
10	11.3 Responsabilités utilisateurs	Utilisation du mot de passe	Demander aux utilisateurs de respecter les bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe.	x	x		Organisation interne / Système d'accès
11	11.4 Contrôle d'accès au réseau	Authentification des administrateurs	Afin d'accéder aux fonctions d'administration, les administrateurs doivent être authentifiés. L'authentification doit se faire de manière sécurisée (chiffrage des mots de passe, authentification à deux facteurs).		x		Système du prestataire
12	11.4 Contrôle d'accès au réseau	Authentification des utilisateurs	L'authentification des utilisateurs doit se faire de manière sécurisée par un cryptage des mots de passe et une authentification à deux facteurs.		x		Système du prestataire
13	14.1 Aspects de la sécurité de l'information en matière de gestion de l'activité	Plan de continuité de l'activité du prestataire	Le prestataire doit fournir les garanties de continuité de l'activité au travers d'un plan de continuité de l'activité. Ce PCA doit prendre en compte les exigences en matière de sécurité de l'information, les évènements pouvant être à l'origine d'interruption des processus métier, les mesures de restauration et de maintien de la disponibilité du système d'information, ainsi que la mise à l'essai dudit plan de continuité de l'activité.	x		x	Système du prestataire

Niveau de risque après application des mesures de sécurité existantes

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	~~4. Intolérable~~
Gravité	1. Négligeable	2. Limitée	**3. Importante**	~~4. Critique~~
Vraisemblance	1. Minime	**2. Significative**	3. Forte	~~4. Maximale~~

Mesures de sécurité complémentaires

N°	Thème ISO 27002	Mesures de sécurité	Description	Prévention	Protection	Récupération	Bien support
2	8.2 Pendant la durée du contrat	Sensibilisation, qualification et formations en matière de sécurité de l'information	Le personnel interne doit être formé aux bonnes pratiques de sécurité. Il doit avoir un niveau de sensibilisation pertinent pour ses fonctions. Cela passe par des sessions de formation et des missives d'information concernant la sécurité.	x	x		Organisation interne

3	8.2 Pendant la durée du contrat	Procédures disciplinaires	Mettre en place un processus disciplinaire clair pour toute ayant enfreint les règles de sécurité pour réduire les risques d'influence et de corruption. Par exemple, les sanctions peuvent être précisées dans une charte définissant les engagements de responsabilités.	x	x		Organisation interne
4	8.3 Fin ou modification de contrat	Retrait des droits d'accès	Les droits d'accès de tout utilisateur ou administrateur aux données et aux logiciels doivent être supprimés en fin de contrat ou doivent être modifiés en cas de changement de contrat ou de responsabilités.	x			Organisation interne
5	9.2 Sécurité du matériel	Mise au rebut ou recyclage sécurisé du matériel	Vérifier tout le matériel contenant des supports de stockage pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut. Le prestataire devra préciser les mesures mises en œuvre pour assurer la mise au rebut de ses matériels.	x	x		Système du prestataire
6	10.2 Gestion de la prestation de service par un tiers	Prestation de service et contrat	S'assurer que les mesures de sécurité, les définitions du service et les niveaux de prestation prévus dans l'accord de prestation de service tiers sont mis en œuvre, appliqués et tenus à jour par le tiers. Notamment, le contrat de prestation de service doit inclure les éléments liés à la journalisation d'évènements, au suivi du service hébergé (mise à jour, maintenances, sauvegardes…), aux modalités de prévention d'une attaque et à la réaction suite à un incident.				Système du prestataire
8	10.2 Gestion de la prestation de service par un tiers	Gestion des modifications dans les services tiers	Gérer les changements effectués dans la prestation de service, comprenant le maintien et l'amélioration des politiques, procédures et mesures existantes. Notamment, le contrat doit permettre la validation des choix du prestataire lors de la mise en œuvre de nouvelles solutions logicielles ou matérielles (pour éviter la perte de sécurité).	x	x		Système du prestataire
10	10.5 Sauvegarde	Sauvegarde des informations - backups	Le prestataire doit prendre toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé. Il doit notamment effectuer un double exemplaire des sauvegardes et doit les conserver dans des locaux physiquement séparés.	x	x	x	Système du prestataire
11	10.10 Surveillance	Protection des informations journalisées	Protection des équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés. Analyser les journaux à l'aide d'un logiciel de contrôle de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
12	10.10 Surveillance	Journal administrateur et journal des opérations	La journalisation des opérations des administrateurs permet de garder une trace des actions des administrateurs.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
13	10.10 Surveillance	Rapports de défaut	Journaliser et analyser les éventuels défauts et prendre les mesures appropriées.		x	x	Système d'accès / Système du prestataire / Système d'accès du prestataire
14	10.10 Surveillance	Audit de la passerelle d'accès au cloud	La passerelle d'accès au cloud doit être soumise à un audit régulier (annuel) pour vérifier que les mesures de sécurité sont effectives et en adéquation avec les objectifs de sécurité.	x			Système d'accès
15	11.4 Contrôle d'accès au réseau	Protection des ports de diagnostic et de configuration à distance	Le prestataire doit contrôler l'accès physique et logique aux ports de diagnostic et de configuration à distance.	x	x		Système du prestataire / Système d'accès du prestataire
16	11.4 Contrôle d'accès au réseau	Mesure relative à la connexion réseau	Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme du prestataire, il convient de vérifier que le prestataire restreigne la capacité de connexion réseau des utilisateurs, conformément à la politique de contrôle d'accès et les exigences relatives aux applications de gestion.	x	x		Système d'accès du prestataire
17	11.4 Contrôle d'accès au réseau	Contrôle du routage réseau interne	S'assurer que l'organisation mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		Système d'accès
18	11.4 Contrôle d'accès au réseau	Contrôle du routage réseau du prestataire	S'assurer que le prestataire mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		Système d'accès du prestataire
19	12.3 Mesures cryptographiques	Politique d'utilisation des mesures cryptographiques	Elaboration et mise en œuvre d'une politique d'utilisation des mesures cryptographiques en vue de protéger l'information. Par exemple, employer un logiciel de chiffrement des données externalisées.	x			Système du prestataire
20	12.3 Mesures cryptographiques	Chiffrement des flux	Les flux contenant des informations sensibles ou à caractère personnel doivent être chiffrées.	x			Système d'accès
21	12.3 Mesures cryptographiques	Gestion des clés	Une procédure de gestion des clés doit venir à l'appui de la politique de l'organisme en matière de chiffrement.	x			Système du prestataire / Système d'accès
22	12.6 Gestion des vulnérabilités techniques	Mesures relatives aux vulnérabilités techniques	Le prestataire doit tenir informé l'organisation (assureur) en temps voulu de toute vulnérabilité technique des systèmes d'information en exploitation, évaluer l'exposition de l'organisation auxdites vulnérabilités et entreprendre les actions appropriées pour traiter le risque associé. Cette démarche doit être formalisée	x			Système du prestataire

			dans le contrat de service.				
23	15.1 Conformité avec les exigences légales	Protection des données et confidentialité des informations relatives à la vie privée	Le prestataire doit satisfaire les exigences de protection et de confidentialité des données à caractère personnel telles que l'exigent la législation ou les réglementations applicables. Le transfert des données à caractère personnel en dehors des frontières de l'Union européenne est réglementé par la directive européenne 95/46/CE et la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.		x		Système du prestataire
24		Hébergement non mutualisé	L'hébergement doit être réalisé sur une ou plusieurs machines spécifiques (non mutualisé). Ainsi, les données de l'organisation (assureur) ne risquent pas de subir les conséquences d'une activité frauduleuse d'un autre client du cloud. Les problèmes de compartimentation sont de plus écartés.	x			Système du prestataire
25	15.1 Conformité avec les exigences légales	Localisation des données	Le prestataire doit être en mesure d'indiquer la localisation des données pour informer l'organisation	x			Système du prestataire

Niveau de risque après application des mesures de sécurité complémentaires

Niveau de risque	**1. Négligeable**	2. Limité	~~3. Significatif~~	4. Intolérable
Gravité	**1. Négligeable**	2. Limitée	~~3. Importante~~	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

4.1.2 Altération des données de déclaration de sinistre

Scénarios décrits dans les documents (ANSSI et ENISA)

Bien(s) support(s)	Scénario(s) de menace
Personnel interne et personnel du prestataire	La répartition des rôles entre le personnel interne et celui du Cloud Provider n'est pas claire et provoque des conflits pouvant compromettre l'intégrité des données.
Système d'accès du prestataire – Réseau du prestataire	Un pirate ou un employé malveillant réalise une attaque de type Man in the Middle et altère les données circulant sur le réseau du prestataire.
Système du prestataire – Logiciel d'administration du prestataire	Les données de plusieurs sociétés sont stockées sur un même support : leur mauvaise séparation entraîne une altération non-intentionnelle des données par un utilisateur d'une autre société.

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de déclaration de sinistre					
ER2	Altération des données	Intègre	• Pirate • Employé du prestataire peu sérieux • Employé peu sérieux • Hébergeur/Faille dans l'application	• Impossibilité de remplir les obligations légales • Impossibilité d'assurer le traitement • Perte de confiance vis-à-vis des clients • Non-conformité aux labels de sécurité	3. Importante

Résultat obtenu par le logiciel

Bien support	Scénarios de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système d'accès (SYS_AIN)	Menace sur le réseau internet causant une altération	I	• Pirate • Concurrent • Employé malveillant	• M13 RSX-USG Attaque du milieu sur un canal informatique	• Attaque de type Man in the Middle	3. Forte
Système du prestataire (SYS_EXT)	Menace sur le système du prestataire causant une altération	I	• Employé du prestataire peu sérieux • Employé du prestataire malveillant • Pirate • Hébergeur/Faille dans l'application	• M7 LOG-USG Détournement de l'usage prévu d'un logiciel • M11 LOG-MOD Modification d'un logiciel	• Données rendues accessibles à d'autres utilisateurs du cloud	3. Forte
Système d'accès du prestataire (SYS_APR)	Menace sur le réseau du prestataire causant une altération	I	• Pirate • Employé du prestataire malveillant	• M13 RSX-USG Attaque du milieu sur un canal informatique • M11 LOG-MOD Modification d'un logiciel	• Attaque de type Man in the Middle • Changement des données du portail d'accès au cloud	3. Forte
Organisation interne (ORG_INT)	Menace sur l'organisation interne causant une altération	I	• Employé peu sérieux	• M21 PER-DEP Surcharge des capacités d'une personne	• Mauvaise répartition des rôles entre le personnel interne et le personnel du prestataire	1. Minime
Organisation du prestataire (ORG_PRE)	Menace sur l'organisation du prestataire causant une	I	• Employé peu sérieux	• M21 PER-DEP Surcharge des capacités d'une personne	• Mauvaise répartition des rôles entre le personnel interne et le personnel du prestataire	1. Minime

	altération					

Menace	Vulnérabilités	Pré-requis	Vraisemblance
Attaque de type Man in the Middle	• Possibilité de falsification du service appelé • Routage altérable	• Accès à la table de routage • Accès aux utilisateurs	3. Forte
Données rendues accessibles à d'autres utilisateurs du cloud	• Mauvaise compartimentation du logiciel	• Serveurs partagés (cloud public) ou réutilisés	2. Significative
Changement des données du portail d'accès au cloud	• Données du portail d'accès modifiables • Données du portail d'accès accessibles avec les droits adéquats	• Accès physique ou logique au portail d'accès • Connaissance de l'existence du portail d'accès	3. Forte
Mauvaise répartition des rôles entre le personnel interne et le personnel du prestataire	• Manque de compétence du personnel • Négligence du personnel	• Partage de l'administration entre le personnel interne et le personnel du prestataire	1. Minime

Niveau de risque avant application des mesures

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	2. Significative	**3. Forte**	4. Maximale

Mesures de sécurité existantes

N°	Thème ISO 27002	Mesures de sécurité existantes	Description	Prévention	Protection	Récupération	Bien support
1	9.1 Zones sécurisée	Périmètre de sécurité physique	Protéger les zones contenant des informations et des moyens de traitement de l'information par des périmètres de sécurité. Les serveurs doivent être inaccessibles par des personnes non autorisées et donc dans des salles hautement sécurisées.	x	x		Système du prestataire
2	9.1 Zones sécurisée	Contrôle physique des accès	Protéger les zones sécurisées pas des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité soit admis. Le prestataire doit donc surveiller et contrôler les accès aux datacenters et doit s'assurer que le personnel de maintenance ou de support ne peut menacer la sécurité des données, des matériels ou des logiciels.	X	x		Système du prestataire
5	9.2 Sécurité du matériel	Sécurité du câblage	Protéger les câbles électriques ou de télécommunications transportant des données contre toute interception ou dommage.		x		Système d'accès du prestataire
6	10.7 Manipulation des supports	Sécurité de la documentation système	La documentation décrivant l'ensemble du système doit être gardée avec un niveau de sécurité suffisant pour ne pas permettre à des personnes malveillantes d'avoir une connaissance poussée de l'architecture (mesures de « diffusion restreinte » systématiques).		x		Organisation interne / Organisation du prestataire
7	11.2 Gestion de l'accès utilisateur	Gestion des privilèges	Restreindre et contrôler l'attribution et l'utilisation des privilèges (gestion des habilitations).	x	x		Organisation interne
8	11.2 Gestion de l'accès utilisateur	Enregistrement des utilisateurs	Définir une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à accorder et à supprimer l'accès au cloud ou à son administration.	x	x		Organisation interne
9	11.2 Gestion de l'accès utilisateur	Gestion du mot de passe utilisateur	L'attribution de mots de passe doit être réalisée dans le cadre d'un processus formel.		x		Organisation interne / Système d'accès
10	11.3 Responsabilités utilisateurs	Utilisation du mot de passe	Demander aux utilisateurs de respecter les bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe.	x	x		Organisation interne / Système d'accès
11	11.4 Contrôle d'accès au réseau	Authentification des administrateurs	Afin d'accéder aux fonctions d'administration, les administrateurs doivent être authentifiés. L'authentification doit se faire de manière sécurisée (chiffrage des mots de passe, authentification à deux facteurs).		x		Système du prestataire
12	11.4 Contrôle d'accès au réseau	Authentification des utilisateurs	L'authentification des utilisateurs doit se faire de manière sécurisée par un cryptage des mots de passe et une authentification à deux facteurs.		x		Système du prestataire
13	14.1 Aspects de la sécurité de l'information en matière de gestion de l'activité	Plan de continuité de l'activité du prestataire	Le prestataire doit fournir les garanties de continuité de l'activité au travers d'un plan de continuité de l'activité. Ce PCA doit prendre en compte les exigences en matière de sécurité de l'information, les évènements pouvant être à l'origine d'interruption des processus métier, les mesures de restauration et de maintien de la disponibilité du système d'information, ainsi que la mise à l'essai dudit plan de continuité de l'activité.	x		x	Système du prestataire

Niveau de risque après application des mesures de sécurité existantes

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable

Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

Mesures de sécurité complémentaires

N°	Thème ISO 27002	Mesures de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	6.1 Organisation interne	Attribution des responsabilités en matière de sécurité de l'information	Il convient de définir clairement toutes les responsabilités en matière de sécurité de l'information. La répartition des responsabilités entre le personnel interne et le personnel du prestataire doit être formalisée et respectée.	x			Organisation interne / Organisation externe
2	8.2 Pendant la durée du contrat	Sensibilisation, qualification et formations en matière de sécurité de l'information	Le personnel interne doit être formé aux bonnes pratiques de sécurité. Il doit avoir un niveau de sensibilisation pertinent pour ses fonctions. Cela passe par des sessions de formation et des missives d'information concernant la sécurité.	x	x		Organisation interne
3	8.2 Pendant la durée du contrat	Procédures disciplinaires	Mettre en place un processus disciplinaire clair pour toute ayant enfreint les règles de sécurité pour réduire les risques d'influence et de corruption. Par exemple, les sanctions peuvent être précisées dans une charte définissant les engagements de responsabilités.	x	x		Organisation interne
4	8.3 Fin ou modification de contrat	Retrait des droits d'accès	Les droits d'accès de tout utilisateur ou administrateur aux données et aux logiciels doivent être supprimés en fin de contrat ou doivent être modifiés en cas de changement de contrat ou de responsabilités.	x			Organisation interne
6	10.2 Gestion de la prestation de service par un tiers	Prestation de service et contrat	S'assurer que les mesures de sécurité, les définitions du service et les niveaux de prestation prévus dans l'accord de prestation de service tiers sont mis en œuvre, appliqués et tenus à jour par le tiers. Notamment, le contrat de prestation de service doit inclure les éléments liés à la journalisation d'évènements, au suivi du service hébergé (mise à jour, maintenances, sauvegardes…), aux modalités de prévention d'une attaque et à la réaction suite à un incident.				Système du prestataire
10	10.5 Sauvegarde	Sauvegarde des informations - backups	Le prestataire doit prendre toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé. Il doit notamment effectuer un double exemplaire des sauvegardes et doit les conserver dans des locaux physiquement séparés.	x	x	x	Système du prestataire
11	10.10 Surveillance	Protection des informations journalisées	Protection des équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés. Analyser les journaux à l'aide d'un logiciel de contrôle de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
12	10.10 Surveillance	Journal administrateur et journal des opérations	La journalisation des opérations des administrateurs permet de garder une trace des actions des administrateurs.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
13	10.10 Surveillance	Rapports de défaut	Journaliser et analyser les éventuels défauts et prendre les mesures appropriées.		x	x	Système d'accès / Système du prestataire / Système d'accès du prestataire
14	10.10 Surveillance	Audit de la passerelle d'accès au cloud	La passerelle d'accès au cloud doit être soumise à un audit régulier (annuel) pour vérifier que les mesures de sécurité sont effectives et en adéquation avec les objectifs de sécurité.	x			Système d'accès
15	11.4 Contrôle d'accès au réseau	Protection des ports de diagnostic et de configuration à distance	Le prestataire doit contrôler l'accès physique et logique aux ports de diagnostic et de configuration à distance.	x	x		Système du prestataire / Système d'accès du prestataire
16	11.4 Contrôle d'accès au réseau	Mesure relative à la connexion réseau	Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme du prestataire, il convient de vérifier que le prestataire restreigne la capacité de connexion réseau des utilisateurs, conformément à la politique de contrôle d'accès et les exigences relatives aux applications de gestion.	x	x		Système d'accès du prestataire
17	11.4 Contrôle d'accès au réseau	Contrôle du routage réseau interne	S'assurer que l'organisation mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		Système d'accès
18	11.4 Contrôle d'accès au réseau	Contrôle du routage réseau du prestataire	S'assurer que le prestataire mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		Système d'accès du prestataire
19	12.3 Mesures cryptographiqu	Politique d'utilisation des	Elaboration et mise en œuvre d'une politique d'utilisation des mesures cryptographiques en vue de protéger l'information. Par exemple, employer un	x			Système du prestataire

	es	mesures cryptographiques	logiciel de chiffrement des données externalisées.					
20	12.3 Mesures cryptographiques	Chiffrement des flux	Les flux contenant des informations sensibles ou à caractère personnel doivent être chiffrées.	x			Système d'accès
21	12.3 Mesures cryptographiques	Gestion des clés	Une procédure de gestion des clés doit venir à l'appui de la politique de l'organisme en matière de chiffrement.	x			Système du prestataire / Système d'accès
22	12.6 Gestion des vulnérabilités techniques	Mesures relatives aux vulnérabilités techniques	Le prestataire doit tenir informé l'organisation (assureur) en temps voulu de toute vulnérabilité technique des systèmes d'information en exploitation, évaluer l'exposition de l'organisation auxdites vulnérabilités et entreprendre les actions appropriées pour traiter le risque associé. Cette démarche doit être formalisée dans le contrat de service.	x			Système du prestataire
23	15.1 Conformité avec les exigences légales	Protection des données et confidentialité des informations relatives à la vie privée	Le prestataire doit satisfaire les exigences de protection et de confidentialité des données à caractère personnel telles que l'exigent la législation ou les réglementations applicables. Le transfert des données à caractère personnel en dehors des frontières de l'Union européenne est réglementé par la directive européenne 95/46/CE et la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.		x		Système du prestataire
24		Hébergement non mutualisé	L'hébergement doit être réalisé sur une ou plusieurs machines spécifiques (non mutualisé). Ainsi, les données de l'organisation (assureur) ne risquent pas de subir les conséquences d'une activité frauduleuse d'un autre client du cloud. Les problèmes de compartimentation sont de plus écartés.	x			Système du prestataire

Niveau de risque après application des mesures de sécurité complémentaires

Niveau de risque	**1. Négligeable**	2. Limité	~~3. Significatif~~	4. Intolérable
Gravité	**1. Négligeable**	2. Limitée	~~3. Importante~~	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

4.1.3 Indisponibilité des données de déclaration de sinistre

Scénarios décrits dans les documents (ANSSI et ENISA)

Bien(s) support(s)	Scénario(s) de menace
Système d'accès – Réseau internet	Une entreprise tierce mène des activités frauduleuses au sein du même cloud et conduit au blocage d'un lot d'adresses IP incluant celles d'entreprises innocentes.
Système du prestataire – Serveurs du prestataire	Une entreprise tierce mène des activités frauduleuses au sein du même cloud et conduit à la confiscation des serveurs par la Justice.
Système du prestataire – Serveurs du prestataire	Les données étant localisées dans différents pays, un changement de juridiction dans l'un de ces pays peut entrainer la confiscation des serveurs par la Justice.
Système du prestataire – Logiciel d'administration du prestataire	L'administrateur du cloud efface de manière non délibérée tout ou partie des données stockées sur les serveurs.
Système du prestataire – Logiciel d'administration du prestataire	L'administrateur du cloud efface de manière délibérée tout ou partie des données stockées sur les serveurs.
Système du prestataire – Serveurs du prestataire	Crash d'un serveur du cloud.
Système du prestataire – Logiciel d'administration du prestataire	Un bogue logiciel entraîne la perte de tout ou partie des données.
Système du prestataire – Logiciel d'administration du prestataire	Une personne non autorisée accède aux fonctionnalités d'administration du cloud et efface délibérément tout ou partie des données.
Personnel interne et personnel du prestataire	Un pirate utilise les techniques de « social engineering » pour effacer des données.
Système du prestataire – Logiciel d'administration du prestataire	Les données de plusieurs sociétés sont stockées sur un même support : leur mauvaise séparation entraîne une perte de données lors de l'effacement d'autres données.
Système du prestataire – Serveurs du prestataire	Une catastrophe naturelle détruit tout ou partie des données.

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de déclaration de sinistre					
ER3	Indisponibilité des données	24h	• Pirate • Employé du prestataire peu sérieux • Employé du prestataire malveillant • Hébergeur/Faille dans l'application • Entreprise tierce • Changement de juridiction • Panne de serveur • Bogue logiciel • Catastrophe naturelle	• Impossibilité d'assurer le traitement • Perte de confiance vis-à-vis des clients	2. Limitée

Résultat obtenu par le logiciel

Bien support	Scénarios de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système d'accès (SYS_AIN)	Menace sur le réseau internet causant une indisponibilité	D	• Entreprise tierce • Pirate • Concurrent • Employé malveillant • Panne de réseau	• M15 RSX-DEP Saturation du canal informatique • M16 RSX-DET Dégradation d'un canal informatique	• Blocage d'un lot d'adresses IP • Occupation de la bande passante (déni de service) • Rupture du canal d'accès au cloud	4. Maximale
Système du prestataire (SYS_EXT)	Menace sur le système du prestataire causant une indisponibilité	D	• Employé du prestataire peu sérieux • Employé du prestataire malveillant • Décision du cloud provider • Concurrent • Pirate • Hébergeur/Faille dans l'application • Décision de justice • Panne de matériel • Bogue logiciel	• M9 LOG-DEP Dépassement des limites d'un logiciel • M12 LOG-PTE Disparition d'un logiciel • M6 MAT-PTE Perte d'un matériel • M7 LOG-USG Détournement de l'usage prévu d'un logiciel • M4 MAT-PTE	• Surexploitation du système du prestataire • Cessation d'activité du prestataire • Serveurs du prestataire saisis par la justice • Perte ou effacement des données • Changement des données du portail d'accès au cloud	3. Forte

			• Catastrophe naturelle	Détérioration d'un matériel • M11 LOG-MOD Modification d'un logiciel		
Système d'accès du prestataire (SYS_APR)	Menace sur le réseau du prestataire causant une indisponibilité	D	• Pirate • Employé du prestataire malveillant • Panne de réseau	• M15 RSX-DEP Saturation du canal informatique • M16 RSX-DET Dégradation d'un canal informatique	• Perte de liaison entre les serveurs du prestataire	3. Forte
Organisation interne (ORG_INT)	Menace sur l'organisation interne causant une indisponibilité	D	• Employé peu sérieux • Pirate	• M23 PER-MOD Influence sur une personne	• Collecte de données d'accès au SI externalisé • Suppression des données par le personnel sous influence d'un pirate	2. Significative
Organisation du prestataire (ORG_PRE)	Menace sur l'organisation du prestataire causant une indisponibilité	D	• Employé du prestataire peu sérieux • Pirate	• M23 PER-MOD Influence sur une personne	• Collecte de données d'accès au SI externalisé • Suppression des données par le personnel sous influence d'un pirate	2. Significative

Menace	Vulnérabilités	Pré-requis	Vraisemblance
Blocage d'un lot d'adresses IP	• Possibilité d'être impliqué dans les activités frauduleuses d'une entreprise tierce sur le cloud	• Serveurs partagés (cloud public)	3. Forte
Occupation de la bande passante (déni de service)	• Réseau d'accès au cloud unique • Dimensionnement insuffisant de la bande passante	• Accès à la table de routage • Accès aux utilisateurs	2. Significative
Rupture du canal d'accès au cloud	• Réseau d'accès au cloud unique • Dimensionnement insuffisant de la bande passante	• Contrôle insuffisant du matériel • Accès physique au réseau	4. Maximale
Surexploitation du système du prestataire	• Manque de compétence du personnel du prestataire • Négligence du personnel du prestataire	• Ressources allouées par le prestataire insuffisantes	1. Minime
Cessation d'activité du prestataire	• Portabilité des données non assurée	• Fébrilité économique du prestataire	2. Significative
Serveurs du prestataire saisis par la justice	• Juridiction liée à la position géographique des données	• Changement de juridiction dans le pays où sont situés les serveurs Ou • Une entreprise tierce mène des activités frauduleuses sur le cloud Ou • Juridiction relative au stockage des données personnelles	2. Significative
Perte ou effacement des données	• Données accessibles avec les droits adéquats • Matériel peu fiable • Matériel inapproprié aux conditions d'utilisation • Datacenter mal protégé contre les catastrophes naturelles • Mauvaise compartimentation du logiciel	• Privilèges élevés sur l'application Ou • Contrôle insuffisant du matériel Ou • Bogue dans le logiciel utilisé Ou • Datacenter dans une zone à risque de catastrophes naturelles Ou • Serveurs partagés (cloud public)	3. Forte
Changement des données du portail d'accès au cloud	• Données du portail d'accès modifiables • Données du portail d'accès accessibles avec les droits adéquats	• Accès physique ou logique au portail d'accès • Connaissance de l'existence du portail d'accès	3. Forte
Perte de liaison entre les serveurs du prestataire	• Réseau d'accès au cloud unique • Dimensionnement insuffisant de la bande passante	• Accès à la table de routage • Accès aux utilisateurs	3. Forte
Collecte de données d'accès au SI externalisé	• Personne influençable ou manipulable	• Etablissement d'une relation avec la personne	2. Significative
Suppression des données par le personnel sous influence d'un pirate	• Personne influençable ou manipulable	• Etablissement d'une relation avec la personne	2. Significative

Niveau de risque avant application des mesures

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	2. Significative	3. Forte	**4. Maximale**

Mesures de sécurité existantes

N°	Thème ISO 27002	Mesures de sécurité existantes	Description	Prévention	Protection	Récupération	Bien support
1	9.1 Zones sécurisée	Périmètre de sécurité physique	Protéger les zones contenant des informations et des moyens de traitement de l'information par des périmètres de sécurité. Les serveurs doivent être inaccessibles par des personnes non autorisées et donc dans des salles hautement sécurisées.	x	x		Système du prestataire
2	9.1 Zones sécurisée	Contrôle physique des accès	Protéger les zones sécurisées pas des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité soit admis. Le prestataire doit donc surveiller et contrôler les accès aux datacenters et doit s'assurer que le personnel de maintenance ou de support ne peut menacer la sécurité des données, des matériels ou des logiciels.	X	x		Système du prestataire
3	9.1 Zones sécurisée	Protection contre les menaces extérieures et environnementales	Concevoir et appliquer des mesures de protection physiques contre les dommages causés par les incendies, les inondations, les tremblements de terre, les explosions, les troubles civils et autres formes de catastrophes naturelles ou de sinistre provoqués par l'homme. Les datacenters du prestataire devront satisfaire les exigences de sécurité liées à la protection physique des serveurs.	x	X		Système du prestataire
4	9.2 Sécurité du matériel	Services généraux	Protéger le matériel des coupures de courant et autres perturbations dues à une défaillance de services généraux.	x	x	x	Système du prestataire
5	9.2 Sécurité du matériel	Sécurité du câblage	Protéger les câbles électriques ou de télécommunications transportant des données contre toute interception ou dommage.		x		Système d'accès du prestataire
6	10.7 Manipulation des supports	Sécurité de la documentation système	La documentation décrivant l'ensemble du système doit être gardée avec un niveau de sécurité suffisant pour ne pas permettre à des personnes malveillantes d'avoir une connaissance poussée de l'architecture (mesures de « diffusion restreinte » systématiques).		x		Organisation interne / Organisation du prestataire
7	11.2 Gestion de l'accès utilisateur	Gestion des privilèges	Restreindre et contrôler l'attribution et l'utilisation des privilèges (gestion des habilitations).	x	x		Organisation interne
8	11.2 Gestion de l'accès utilisateur	Enregistrement des utilisateurs	Définir une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à accorder et à supprimer l'accès au cloud ou à son administration.	x	x		Organisation interne
9	11.2 Gestion de l'accès utilisateur	Gestion du mot de passe utilisateur	L'attribution de mots de passe doit être réalisée dans le cadre d'un processus formel.		x		Organisation interne / Système d'accès
10	11.3 Responsabilités utilisateurs	Utilisation du mot de passe	Demander aux utilisateurs de respecter les bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe.	x	x		Organisation interne / Système d'accès
11	11.4 Contrôle d'accès au réseau	Authentification des administrateurs	Afin d'accéder aux fonctions d'administration, les administrateurs doivent être authentifiés. L'authentification doit se faire de manière sécurisée (chiffrage des mots de passe, authentification à deux facteurs).		x		Système du prestataire
12	11.4 Contrôle d'accès au réseau	Authentification des utilisateurs	L'authentification des utilisateurs doit se faire de manière sécurisée par un cryptage des mots de passe et une authentification à deux facteurs.		x		Système du prestataire
13	14.1 Aspects de la sécurité de l'information en matière de gestion de l'activité	Plan de continuité de l'activité du prestataire	Le prestataire doit fournir les garanties de continuité de l'activité au travers d'un plan de continuité de l'activité. Ce PCA doit prendre en compte les exigences en matière de sécurité de l'information, les évènements pouvant être à l'origine d'interruption des processus métier, les mesures de restauration et de maintien de la disponibilité du système d'information, ainsi que la mise à l'essai dudit plan de continuité de l'activité.	x		x	Système du prestataire

Niveau de risque après application des mesures de sécurité existantes

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	2. Significative	**3. Forte**	~~4. Maximale~~

Mesures de sécurité complémentaires

N°	Thème ISO 27002	Mesures de sécurité	Description	Prévention	Protection	Récupération	Bien support
2	8.2 Pendant la durée du contrat	Sensibilisation, qualification et formations en matière de sécurité de l'information	Le personnel interne doit être formé aux bonnes pratiques de sécurité. Il doit avoir un niveau de sensibilisation pertinent pour ses fonctions. Cela passe par des sessions de formation et des missives d'information concernant la sécurité.	x	x		Organisation interne
3	8.2 Pendant la	Procédures	Mettre en place un processus disciplinaire clair pour toute ayant enfreint les	x	x		Organisation

	durée du contrat	disciplinaires	règles de sécurité pour réduire les risques d'influence et de corruption. Par exemple, les sanctions peuvent être précisées dans une charte définissant les engagements de responsabilités.				interne
4	8.3 Fin ou modification de contrat	Retrait des droits d'accès	Les droits d'accès de tout utilisateur ou administrateur aux données et aux logiciels doivent être supprimés en fin de contrat ou doivent être modifiés en cas de changement de contrat ou de responsabilités.	x			Organisation interne
6	10.2 Gestion de la prestation de service par un tiers	Prestation de service et contrat	S'assurer que les mesures de sécurité, les définitions du service et les niveaux de prestation prévus dans l'accord de prestation de service tiers sont mis en œuvre, appliqués et tenus à jour par le tiers. Notamment, le contrat de prestation de service doit inclure les éléments liés à la journalisation d'évènements, au suivi du service hébergé (mise à jour, maintenances, sauvegardes…), aux modalités de prévention d'une attaque et à la réaction suite à un incident.				Système du prestataire
7	10.2 Gestion de la prestation de service par un tiers	Clause contractuelle de restitution des données	Le contrat de prestation de service doit préciser les conditions de restitution des données (conditions, délais, formats) pour permettre le rapatriement des données ou le changement de prestataire sans interruption de service.	x		x	Système du prestataire
8	10.2 Gestion de la prestation de service par un tiers	Gestion des modifications dans les services tiers	Gérer les changements effectués dans la prestation de service, comprenant le maintien et l'amélioration des politiques, procédures et mesures existantes. Notamment, le contrat doit permettre la validation des choix du prestataire lors de la mise en œuvre de nouvelles solutions logicielles ou matérielles (pour éviter la perte de sécurité).	x	x		Système du prestataire
9	10.3 Planification et acceptation du système	Dimensionnement	Les ressources doivent correspondre aux besoins. Il est nécessaire de faire des projections et des tests de performance pour connaître les limites du système et pouvoir anticiper toute surcharge. Ainsi, le prestataire doit s'assurer que les ressources allouées aux différents utilisateurs du service sont suffisantes pour couvrir les besoins.	x			Système d'accès / Système du prestataire / Système d'accès du prestataire
10	10.5 Sauvegarde	Sauvegarde des informations - backups	Le prestataire doit prendre toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé. Il doit notamment effectuer un double exemplaire des sauvegardes et doit les conserver dans des locaux physiquement séparés.	x	x	x	Système du prestataire
11	10.10 Surveillance	Protection des informations journalisées	Protection des équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés. Analyser les journaux à l'aide d'un logiciel de contrôle de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
12	10.10 Surveillance	Journal administrateur et journal des opérations	La journalisation des opérations des administrateurs permet de garder une trace des actions des administrateurs.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
13	10.10 Surveillance	Rapports de défaut	Journaliser et analyser les éventuels défauts et prendre les mesures appropriées.		x	x	Système d'accès / Système du prestataire / Système d'accès du prestataire
14	10.10 Surveillance	Audit de la passerelle d'accès au cloud	La passerelle d'accès au cloud doit être soumise à un audit régulier (annuel) pour vérifier que les mesures de sécurité sont effectives et en adéquation avec les objectifs de sécurité.	x			Système d'accès
15	11.4 Contrôle d'accès au réseau	Protection des ports de diagnostic et de configuration à distance	Le prestataire doit contrôler l'accès physique et logique aux ports de diagnostic et de configuration à distance.	x	x		Système du prestataire / Système d'accès du prestataire
16	11.4 Contrôle d'accès au réseau	Mesure relative à la connexion réseau	Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme du prestataire, il convient de vérifier que le prestataire restreigne la capacité de connexion réseau des utilisateurs, conformément à la politique de contrôle d'accès et les exigences relatives aux applications de gestion.	x	x		Système d'accès du prestataire
17	11.4 Contrôle d'accès au réseau	Contrôle du routage réseau interne	S'assurer que l'organisation mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		Système d'accès
18	11.4 Contrôle d'accès au réseau	Contrôle du routage réseau du prestataire	S'assurer que le prestataire mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		Système d'accès du prestataire
22	12.6 Gestion des vulnérabilités techniques	Mesures relatives aux vulnérabilités techniques	Le prestataire doit tenir informé l'organisation (assureur) en temps voulu de toute vulnérabilité technique des systèmes d'information en exploitation, évaluer l'exposition de l'organisation auxdites vulnérabilités et entreprendre les actions appropriées pour traiter le risque associé. Cette démarche doit être formalisée dans le contrat de service.	x			Système du prestataire
24		Hébergement non mutualisé	L'hébergement doit être réalisé sur une ou plusieurs machines spécifiques (non mutualisé). Ainsi, les données de l'organisation (assureur) ne risquent pas de subir les conséquences d'une activité frauduleuse d'un autre client du cloud. Les problèmes de compartimentation sont de plus écartés.	x			Système du prestataire

25	15.1 Conformité avec les exigences légales	Localisation des données	Le prestataire doit être en mesure d'indiquer la localisation des données pour informer l'organisation	x			Système du prestataire

Niveau de risque après application des mesures de sécurité complémentaires

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

4.1.4 Divulgation des données de sécurité

Scénarios décrits dans les documents (ANSSI et ENISA)

Bien(s) support(s)	Scénario(s) de menace
Système du prestataire – Portail d'accès	Un pirate récupère les données du portail d'accès permettant un accès à tout le système

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de sécurité					
ER4	Divulgation des données de sécurité	Privé	• Pirate	• Mise en péril du système d'information externalisé • Impossibilité de remplir les obligations légales • Non-conformité aux labels de sécurité • Perte de notoriété • Perte de confiance vis-à-vis des clients • Chute de valeur en bourse	4. Critique

Résultat obtenu par le logiciel

Bien support	Scénarios de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système d'accès (SYS_AIN)	Menace sur le réseau internet causant une compromission	C	• Pirate • Concurrent • Employé malveillant	• M14 RSX-ESP Ecoute passive d'un canal informatique	• Acquisition de données par écoute passive	3. Forte
Système d'accès du prestataire (SYS_APR)	Menace sur le réseau du prestataire causant une compromission	C	• Pirate • Employé du prestataire malveillant	• M14 RSX-ESP Ecoute passive d'un canal informatique	• Acquisition de données par écoute passive entre les serveurs du prestataire	3. Forte
Organisation interne (ORG_INT)	Menace sur l'organisation interne causant une compromission	C	• Employé malveillant	• M23 PER-MOD Influence sur une personne	• L'employé se venge	3. Forte
Organisation du prestataire (ORG_PRE)	Menace sur l'organisation du prestataire causant une compromission	C	• Employé malveillant	• M23 PER-MOD Influence sur une personne	• L'employé se venge	3. Forte

Menace	Vulnérabilités	Pré-requis	Vraisemblance
Acquisition de données par écoute passive	• Réseau perméable • Données transmises interprétables	• Accès à la table de routage • Accès aux utilisateurs	3. Forte
Acquisition de données par écoute passive entre les serveurs du prestataire	• Perméabilité du réseau • Données observables lors du transfert	• Accès à la table de routage • Accès aux utilisateurs	3. Forte
L'employé se venge	• Personne influençable ou manipulable	• Privilèges élevés sur l'application • Motivation de la vengeance	3. Forte

Niveau de risque avant application des mesures

Niveau de risque	1. Négligeable	2. Limité	3. Significatif	**4. Intolérable**
Gravité	1. Négligeable	2. Limitée	3. Importante	**4. Critique**
Vraisemblance	1. Minime	2. Significative	**3. Forte**	4. Maximale

Mesures de sécurité existantes

N°	Thème ISO 27002	Mesures de sécurité existantes	Description	Prévention	Protection	Récupération	Bien support
1	9.1 Zones sécurisée	Périmètre de sécurité physique	Protéger les zones contenant des informations et des moyens de traitement de l'information par des périmètres de sécurité. Les serveurs doivent être inaccessibles par des personnes non autorisées et donc dans des salles hautement sécurisées.	x	x		Système du prestataire
2	9.1 Zones sécurisée	Contrôle physique des accès	Protéger les zones sécurisées pas des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité soit admis. Le prestataire doit donc	X	x		Système du prestataire

			surveiller et contrôler les accès aux datacenters et doit s'assurer que le personnel de maintenance ou de support ne peut menacer la sécurité des données, des matériels ou des logiciels.				
5	9.2 Sécurité du matériel	Sécurité du câblage	Protéger les câbles électriques ou de télécommunications transportant des données contre toute interception ou dommage.		x		Système d'accès du prestataire
6	10.7 Manipulation des supports	Sécurité de la documentation système	La documentation décrivant l'ensemble du système doit être gardée avec un niveau de sécurité suffisant pour ne pas permettre à des personnes malveillantes d'avoir une connaissance poussée de l'architecture (mesures de « diffusion restreinte » systématiques).		x		Organisation interne / Organisation du prestataire
7	11.2 Gestion de l'accès utilisateur	Gestion des privilèges	Restreindre et contrôler l'attribution et l'utilisation des privilèges (gestion des habilitations).	x	x		Organisation interne
8	11.2 Gestion de l'accès utilisateur	Enregistrement des utilisateurs	Définir une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à accorder et à supprimer l'accès au cloud ou à son administration.	x	x		Organisation interne
9	11.2 Gestion de l'accès utilisateur	Gestion du mot de passe utilisateur	L'attribution de mots de passe doit être réalisée dans le cadre d'un processus formel.		x		Organisation interne / Système d'accès
10	11.3 Responsabilités utilisateurs	Utilisation du mot de passe	Demander aux utilisateurs de respecter les bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe.	x	x		Organisation interne / Système d'accès
11	11.4 Contrôle d'accès au réseau	Authentification des administrateurs	Afin d'accéder aux fonctions d'administration, les administrateurs doivent être authentifiés. L'authentification doit se faire de manière sécurisée (chiffrage des mots de passe, authentification à deux facteurs).		x		Système du prestataire
12	11.4 Contrôle d'accès au réseau	Authentification des utilisateurs	L'authentification des utilisateurs doit se faire de manière sécurisée par un cryptage des mots de passe et une authentification à deux facteurs.		x		Système du prestataire

Niveau de risque après application des mesures de sécurité existantes

Niveau de risque	1. Négligeable	2. Limité	3. Significatif	**4. Intolérable**
Gravité	1. Négligeable	2. Limitée	3. Importante	**4. Critique**
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

Mesures de sécurité complémentaires

N°	Thème ISO 27002	Mesures de sécurité	Description	Prévention	Protection	Récupération	Bien support
2	8.2 Pendant la durée du contrat	Sensibilisation, qualification et formations en matière de sécurité de l'information	Le personnel interne doit être formé aux bonnes pratiques de sécurité. Il doit avoir un niveau de sensibilisation pertinent pour ses fonctions. Cela passe par des sessions de formation et des missives d'information concernant la sécurité.	x	x		Organisation interne
3	8.2 Pendant la durée du contrat	Procédures disciplinaires	Mettre en place un processus disciplinaire clair pour toute ayant enfreint les règles de sécurité pour réduire les risques d'influence et de corruption. Par exemple, les sanctions peuvent être précisées dans une charte définissant les engagements de responsabilités.	x	x		Organisation interne
4	8.3 Fin ou modification de contrat	Retrait des droits d'accès	Les droits d'accès de tout utilisateur ou administrateur aux données et aux logiciels doivent être supprimés en fin de contrat ou doivent être modifiés en cas de changement de contrat ou de responsabilités.	x			Organisation interne
8	10.2 Gestion de la prestation de service par un tiers	Gestion des modifications dans les services tiers	Gérer les changements effectués dans la prestation de service, comprenant le maintien et l'amélioration des politiques, procédures et mesures existantes. Notamment, le contrat doit permettre la validation des choix du prestataire lors de la mise en œuvre de nouvelles solutions logicielles ou matérielles (pour éviter la perte de sécurité).	x	x		Système du prestataire
10	10.5 Sauvegarde	Sauvegarde des informations - backups	Le prestataire doit prendre toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé. Il doit notamment effectuer un double exemplaire des sauvegardes et doit les conserver dans des locaux physiquement séparés.	x	x	x	Système du prestataire
11	10.10 Surveillance	Protection des informations journalisées	Protection des équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés. Analyser les journaux à l'aide d'un logiciel de contrôle de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
12	10.10 Surveillance	Journal administrateur et journal des opérations	La journalisation des opérations des administrateurs permet de garder une trace des actions des administrateurs.	x	x		Système d'accès / Système du prestataire / Système

							d'accès du prestataire
13	10.10 Surveillance	Rapports de défaut	Journaliser et analyser les éventuels défauts et prendre les mesures appropriées.		x	x	Système d'accès / Système du prestataire / Système d'accès du prestataire
14	10.10 Surveillance	Audit de la passerelle d'accès au cloud	La passerelle d'accès au cloud doit être soumise à un audit régulier (annuel) pour vérifier que les mesures de sécurité sont effectives et en adéquation avec les objectifs de sécurité.	x			Système d'accès
15	11.4 Contrôle d'accès au réseau	Protection des ports de diagnostic et de configuration à distance	Le prestataire doit contrôler l'accès physique et logique aux ports de diagnostic et de configuration à distance.	x	x		Système du prestataire / Système d'accès du prestataire
16	11.4 Contrôle d'accès au réseau	Mesure relative à la connexion réseau	Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme du prestataire, il convient de vérifier que le prestataire restreigne la capacité de connexion réseau des utilisateurs, conformément à la politique de contrôle d'accès et les exigences relatives aux applications de gestion.	x	x		Système d'accès du prestataire
17	11.4 Contrôle d'accès au réseau	Contrôle du routage réseau interne	S'assurer que l'organisation mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		Système d'accès
18	11.4 Contrôle d'accès au réseau	Contrôle du routage réseau du prestataire	S'assurer que le prestataire mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		Système d'accès du prestataire
20	12.3 Mesures cryptographiques	Chiffrement des flux	Les flux contenant des informations sensibles ou à caractère personnel doivent être chiffrées.	x			Système d'accès
21	12.3 Mesures cryptographiques	Gestion des clés	Une procédure de gestion des clés doit venir à l'appui de la politique de l'organisme en matière de chiffrement.	x			Système du prestataire / Système d'accès
22	12.6 Gestion des vulnérabilités techniques	Mesures relatives aux vulnérabilités techniques	Le prestataire doit tenir informé l'organisation (assureur) en temps voulu de toute vulnérabilité technique des systèmes d'information en exploitation, évaluer l'exposition de l'organisation auxdites vulnérabilités et entreprendre les actions appropriées pour traiter le risque associé. Cette démarche doit être formalisée dans le contrat de service.	x			Système du prestataire
23	15.1 Conformité avec les exigences légales	Protection des données et confidentialité des informations relatives à la vie privée	Le prestataire doit satisfaire les exigences de protection et de confidentialité des données à caractère personnel telles que l'exigent la législation ou les réglementations applicables. Le transfert des données à caractère personnel en dehors des frontières de l'Union européenne est réglementé par la directive européenne 95/46/CE et la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.		x		Système du prestataire

Niveau de risque après application des mesures de sécurité complémentaires

Niveau de risque	1. Négligeable	**2. Limité**	3. Significatif	~~4. Intolérable~~
Gravité	1. Négligeable	**2. Limitée**	3. Importante	~~4. Critique~~
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

4.1.5 Altération des données de sécurité

Scénarios décrits dans les documents (ANSSI et ENISA)

Bien(s) support(s)	Scénario(s) de menace
Système du prestataire – Portail d'accès	Un administrateur fonctionnel interne ou un pirate modifie le référentiel des identités et des droits pour permettre l'accès au système à des personnes non autorisées.

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de sécurité					
ER5	Altération des données de sécurité	Intègre	• Pirate • Employé peu sérieux • Employé malveillant	• Perte de contrôle sur le système d'information externalisé • Impossibilité d'assurer le traitement	3. Importante

Résultat obtenu par le logiciel

Bien support	Scénarios de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système d'accès (SYS_AIN)	Menace sur le réseau internet causant une altération	I	• Pirate • Concurrent • Employé malveillant	• M13 RSX-USG Attaque du milieu sur un canal informatique	• Attaque de type Man in the Middle	3. Forte
Système d'accès du prestataire (SYS_APR)	Menace sur le réseau du prestataire causant une altération	I	• Pirate • Employé du prestataire malveillant	• M13 RSX-USG Attaque du milieu sur un canal informatique • M11 LOG-MOD Modification d'un logiciel	• Attaque de type Man in the Middle • Changement des données du portail d'accès au cloud	3. Forte
Organisation interne (ORG_INT)	Menace sur l'organisation interne causant une altération	I	• Employé peu sérieux	• M21 PER-DEP Surcharge des capacités d'une personne	• Mauvaise répartition des rôles entre le personnel interne et le personnel du prestataire	1. Minime
Organisation du prestataire (ORG_PRE)	Menace sur l'organisation du prestataire causant une altération	I	• Employé peu sérieux	• M21 PER-DEP Surcharge des capacités d'une personne	• Mauvaise répartition des rôles entre le personnel interne et le personnel du prestataire	1. Minime

Menace	Vulnérabilités	Pré-requis	Vraisemblance
Attaque de type Man in the Middle	• Possibilité de falsification du service appelé • Routage altérable	• Accès à la table de routage • Accès aux utilisateurs	3. Forte
Changement des données du portail d'accès au cloud	• Données du portail d'accès modifiables • Données du portail d'accès accessibles avec les droits adéquats	• Accès physique ou logique au portail d'accès • Connaissance de l'existence du portail d'accès	3. Forte
Mauvaise répartition des rôles entre le personnel interne et le personnel du prestataire	• Manque de compétence du personnel • Négligence du personnel	• Partage de l'administration entre le personnel interne et le personnel du prestataire	1. Minime

Niveau de risque avant application des mesures

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	2. Significative	**3. Forte**	4. Maximale

Mesures de sécurité existantes

N°	Thème ISO 27002	Mesures de sécurité existantes	Description	Prévention	Protection	Récupération	Bien support
1	9.1 Zones sécurisée	Périmètre de sécurité physique	Protéger les zones contenant des informations et des moyens de traitement de l'information par des périmètres de sécurité. Les serveurs doivent être inaccessibles par des personnes non autorisées et donc dans des salles hautement sécurisées.	x	x		Système du prestataire
2	9.1 Zones sécurisée	Contrôle physique des accès	Protéger les zones sécurisées pas des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité soit admis. Le prestataire doit donc surveiller et contrôler les accès aux datacenters et doit s'assurer que le personnel de maintenance ou de support ne peut menacer la sécurité des	X	x		Système du prestataire

			données, des matériels ou des logiciels.				
5	9.2 Sécurité du matériel	Sécurité du câblage	Protéger les câbles électriques ou de télécommunications transportant des données contre toute interception ou dommage.		x		Système d'accès du prestataire
6	10.7 Manipulation des supports	Sécurité de la documentation système	La documentation décrivant l'ensemble du système doit être gardée avec un niveau de sécurité suffisant pour ne pas permettre à des personnes malveillantes d'avoir une connaissance poussée de l'architecture (mesures de « diffusion restreinte » systématiques).		x		Organisation interne / Organisation du prestataire
7	11.2 Gestion de l'accès utilisateur	Gestion des privilèges	Restreindre et contrôler l'attribution et l'utilisation des privilèges (gestion des habilitations).	x	x		Organisation interne
8	11.2 Gestion de l'accès utilisateur	Enregistrement des utilisateurs	Définir une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à accorder et à supprimer l'accès au cloud ou à son administration.	x	x		Organisation interne
9	11.2 Gestion de l'accès utilisateur	Gestion du mot de passe utilisateur	L'attribution de mots de passe doit être réalisée dans le cadre d'un processus formel.		x		Organisation interne / Système d'accès
10	11.3 Responsabilités utilisateurs	Utilisation du mot de passe	Demander aux utilisateurs de respecter les bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe.	x	x		Organisation interne / Système d'accès
11	11.4 Contrôle d'accès au réseau	Authentification des administrateurs	Afin d'accéder aux fonctions d'administration, les administrateurs doivent être authentifiés. L'authentification doit se faire de manière sécurisée (chiffrage des mots de passe, authentification à deux facteurs).		x		Système du prestataire
12	11.4 Contrôle d'accès au réseau	Authentification des utilisateurs	L'authentification des utilisateurs doit se faire de manière sécurisée par un cryptage des mots de passe et une authentification à deux facteurs.		x		Système du prestataire

Niveau de risque après application des mesures de sécurité existantes

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

Mesures de sécurité complémentaires

N°	Thème ISO 27002	Mesures de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	6.1 Organisation interne	Attribution des responsabilités en matière de sécurité de l'information	Il convient de définir clairement toutes les responsabilités en matière de sécurité de l'information. La répartition des responsabilités entre le personnel interne et le personnel du prestataire doit être formalisée et respectée.	x			Organisation interne / Organisation externe
2	8.2 Pendant la durée du contrat	Sensibilisation, qualification et formations en matière de sécurité de l'information	Le personnel interne doit être formé aux bonnes pratiques de sécurité. Il doit avoir un niveau de sensibilisation pertinent pour ses fonctions. Cela passe par des sessions de formation et des missives d'information concernant la sécurité.	x	x		Organisation interne
3	8.2 Pendant la durée du contrat	Procédures disciplinaires	Mettre en place un processus disciplinaire clair pour toute ayant enfreint les règles de sécurité pour réduire les risques d'influence et de corruption. Par exemple, les sanctions peuvent être précisées dans une charte définissant les engagements de responsabilités.	x	x		Organisation interne
11	10.10 Surveillance	Protection des informations journalisées	Protection des équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés. Analyser les journaux à l'aide d'un logiciel de contrôle de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
12	10.10 Surveillance	Journal administrateur et journal des opérations	La journalisation des opérations des administrateurs permet de garder une trace des actions des administrateurs.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
13	10.10 Surveillance	Rapports de défaut	Journaliser et analyser les éventuels défauts et prendre les mesures appropriées.		x	x	Système d'accès / Système du prestataire / Système d'accès du prestataire

14	10.10 Surveillance	Audit de la passerelle d'accès au cloud	La passerelle d'accès au cloud doit être soumise à un audit régulier (annuel) pour vérifier que les mesures de sécurité sont effectives et en adéquation avec les objectifs de sécurité.	x			Système d'accès
15	11.4 Contrôle d'accès au réseau	Protection des ports de diagnostic et de configuration à distance	Le prestataire doit contrôler l'accès physique et logique aux ports de diagnostic et de configuration à distance.	x	x		Système du prestataire / Système d'accès du prestataire
16	11.4 Contrôle d'accès au réseau	Mesure relative à la connexion réseau	Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme du prestataire, il convient de vérifier que le prestataire restreigne la capacité de connexion réseau des utilisateurs, conformément à la politique de contrôle d'accès et les exigences relatives aux applications de gestion.	x	x		Système d'accès du prestataire
17	11.4 Contrôle d'accès au réseau	Contrôle du routage réseau interne	S'assurer que l'organisation mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		Système d'accès
18	11.4 Contrôle d'accès au réseau	Contrôle du routage réseau du prestataire	S'assurer que le prestataire mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		Système d'accès du prestataire
20	12.3 Mesures cryptographiques	Chiffrement des flux	Les flux contenant des informations sensibles ou à caractère personnel doivent être chiffrées.	x			Système d'accès
21	12.3 Mesures cryptographiques	Gestion des clés	Une procédure de gestion des clés doit venir à l'appui de la politique de l'organisme en matière de chiffrement.	x			Système du prestataire / Système d'accès

Niveau de risque après application des mesures de sécurité complémentaires

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

4.1.6 Indisponibilité des données de sécurité

Scénarios décrits dans les documents (ANSSI et ENISA)

Bien(s) support(s)	Scénario(s) de menace
Système du prestataire – Portail d'accès	Un pirate ou un employé voulant se venger compromet les mécanismes d'accès au cloud tels que les référentiels d'identité ou les clés de chiffrement

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de sécurité					
ER6	Indisponibilité des données de sécurité	48h	• Pirate • Employé malveillant	• Perte de contrôle sur le système d'information externalisé	2. Limitée

Résultat obtenu par le logiciel

Bien support	Scénarios de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système d'accès (SYS_AIN)	Menace sur le réseau internet causant une indisponibilité	D	• Entreprise tierce • Pirate • Concurrent • Employé malveillant • Panne de réseau	• M15 RSX-DEP Saturation du canal informatique • M16 RSX-DET Dégradation d'un canal informatique	• Blocage d'un lot d'adresses IP • Occupation de la bande passante (déni de service) • Rupture du canal d'accès au cloud	4. Maximale
Système d'accès du prestataire (SYS_APR)	Menace sur le réseau du prestataire causant une indisponibilité	D	• Pirate • Employé du prestataire malveillant • Panne de réseau	• M15 RSX-DEP Saturation du canal informatique • M16 RSX-DET Dégradation d'un canal informatique	• Perte de liaison entre les serveurs du prestataire	3. Forte
Organisation interne (ORG_INT)	Menace sur l'organisation interne causant une indisponibilité	D	• Employé peu sérieux • Pirate	• M23 PER-MOD Influence sur une personne	• Collecte de données d'accès au SI externalisé • Suppression des données par le personnel sous influence d'un pirate	2. Significative
Organisation du prestataire (ORG_PRE)	Menace sur l'organisation du prestataire causant une indisponibilité	D	• Employé du prestataire peu sérieux • Pirate	• M23 PER-MOD Influence sur une personne	• Collecte de données d'accès au SI externalisé • Suppression des données par le personnel sous influence d'un pirate	2. Significative

Menace	Vulnérabilités	Pré-requis	Vraisemblance
Blocage d'un lot d'adresses IP	• Possibilité d'être impliqué dans les activités frauduleuses d'une entreprise tierce sur le cloud	• Serveurs partagés (cloud public)	3. Forte
Occupation de la bande passante (déni de service)	• Réseau d'accès au cloud unique • Dimensionnement insuffisant de la bande passante	• Accès à la table de routage • Accès aux utilisateurs	2. Significative
Rupture du canal d'accès au cloud	• Réseau d'accès au cloud unique • Dimensionnement insuffisant de la bande passante	• Contrôle insuffisant du matériel • Accès physique au réseau	4. Maximale
Perte de liaison entre les serveurs du prestataire	• Réseau d'accès au cloud unique • Dimensionnement insuffisant de la bande passante	• Accès à la table de routage • Accès aux utilisateurs	3. Forte
Collecte de données d'accès au SI externalisé	• Personne influençable ou manipulable	• Etablissement d'une relation avec la personne	2. Significative
Suppression des données par le personnel sous influence d'un pirate	• Personne influençable ou manipulable	• Etablissement d'une relation avec la personne	2. Significative

Niveau de risque avant application des mesures

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	2. Significative	3. Forte	**4. Maximale**

Mesures de sécurité existantes

N°	Thème ISO 27002	Mesures de sécurité existantes	Description	Prévention	Protection	Récupération	Bien support
1	9.1 Zones sécurisée	Périmètre de sécurité physique	Protéger les zones contenant des informations et des moyens de traitement de l'information par des périmètres de sécurité. Les serveurs doivent être inaccessibles par des personnes non autorisées et donc dans des salles hautement sécurisées.	x	x		Système du prestataire
2	9.1 Zones sécurisée	Contrôle physique des accès	Protéger les zones sécurisées pas des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité soit admis. Le prestataire doit donc surveiller et contrôler les accès aux datacenters et doit s'assurer que le personnel de maintenance ou de support ne peut menacer la sécurité des données, des matériels ou des logiciels.	X	x		Système du prestataire
4	9.2 Sécurité du matériel	Services généraux	Protéger le matériel des coupures de courant et autres perturbations dues à une défaillance de services généraux.	x	x	x	Système du prestataire
5	9.2 Sécurité du matériel	Sécurité du câblage	Protéger les câbles électriques ou de télécommunications transportant des données contre toute interception ou dommage.		x		Système d'accès du prestataire
6	10.7 Manipulation des supports	Sécurité de la documentation système	La documentation décrivant l'ensemble du système doit être gardée avec un niveau de sécurité suffisant pour ne pas permettre à des personnes malveillantes d'avoir une connaissance poussée de l'architecture (mesures de « diffusion restreinte » systématiques).		x		Organisation interne / Organisation du prestataire
7	11.2 Gestion de l'accès utilisateur	Gestion des privilèges	Restreindre et contrôler l'attribution et l'utilisation des privilèges (gestion des habilitations).	x	x		Organisation interne
8	11.2 Gestion de l'accès utilisateur	Enregistrement des utilisateurs	Définir une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à accorder et à supprimer l'accès au cloud ou à son administration.	x	x		Organisation interne
9	11.2 Gestion de l'accès utilisateur	Gestion du mot de passe utilisateur	L'attribution de mots de passe doit être réalisée dans le cadre d'un processus formel.		x		Organisation interne / Système d'accès
10	11.3 Responsabilités utilisateurs	Utilisation du mot de passe	Demander aux utilisateurs de respecter les bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe.	x	x		Organisation interne / Système d'accès
11	11.4 Contrôle d'accès au réseau	Authentification des administrateurs	Afin d'accéder aux fonctions d'administration, les administrateurs doivent être authentifiés. L'authentification doit se faire de manière sécurisée (chiffrage des mots de passe, authentification à deux facteurs).		x		Système du prestataire
12	11.4 Contrôle d'accès au réseau	Authentification des utilisateurs	L'authentification des utilisateurs doit se faire de manière sécurisée par un cryptage des mots de passe et une authentification à deux facteurs.		x		Système du prestataire
13	14.1 Aspects de la sécurité de l'information en matière de gestion de l'activité	Plan de continuité de l'activité du prestataire	Le prestataire doit fournir les garanties de continuité de l'activité au travers d'un plan de continuité de l'activité. Ce PCA doit prendre en compte les exigences en matière de sécurité de l'information, les évènements pouvant être à l'origine d'interruption des processus métier, les mesures de restauration et de maintien de la disponibilité du système d'information, ainsi que la mise à l'essai dudit plan de continuité de l'activité.	x		x	Système du prestataire

Niveau de risque après application des mesures de sécurité existantes

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	**2. Significative**	3. Forte	~~4. Maximale~~

Mesures de sécurité complémentaires

N°	Thème ISO 27002	Mesures de sécurité	Description	Prévention	Protection	Récupération	Bien support
2	8.2 Pendant la durée du contrat	Sensibilisation, qualification et formations en matière de sécurité de l'information	Le personnel interne doit être formé aux bonnes pratiques de sécurité. Il doit avoir un niveau de sensibilisation pertinent pour ses fonctions. Cela passe par des sessions de formation et des missives d'information concernant la sécurité.	x	x		Organisation interne
3	8.2 Pendant la durée du contrat	Procédures disciplinaires	Mettre en place un processus disciplinaire clair pour toute ayant enfreint les règles de sécurité pour réduire les risques d'influence et de corruption. Par exemple, les sanctions peuvent être précisées dans une charte définissant les engagements de responsabilités.	x	x		Organisation interne
4	8.3 Fin ou modification de	Retrait des droits d'accès	Les droits d'accès de tout utilisateur ou administrateur aux données et aux logiciels doivent être supprimés en fin de contrat ou doivent être modifiés en cas	x			Organisation interne

	contrat		de changement de contrat ou de responsabilités.				
6	10.2 Gestion de la prestation de service par un tiers	Prestation de service et contrat	S'assurer que les mesures de sécurité, les définitions du service et les niveaux de prestation prévus dans l'accord de prestation de service tiers sont mis en œuvre, appliqués et tenus à jour par le tiers. Notamment, le contrat de prestation de service doit inclure les éléments liés à la journalisation d'évènements, au suivi du service hébergé (mise à jour, maintenances, sauvegardes…), aux modalités de prévention d'une attaque et à la réaction suite à un incident.				Système du prestataire
8	10.2 Gestion de la prestation de service par un tiers	Gestion des modifications dans les services tiers	Gérer les changements effectués dans la prestation de service, comprenant le maintien et l'amélioration des politiques, procédures et mesures existantes. Notamment, le contrat doit permettre la validation des choix du prestataire lors de la mise en œuvre de nouvelles solutions logicielles ou matérielles (pour éviter la perte de sécurité).	x	x		Système du prestataire
9	10.3 Planification et acceptation du système	Dimensionnement	Les ressources doivent correspondre aux besoins. Il est nécessaire de faire des projections et des tests de performance pour connaître les limites du système et pouvoir anticiper toute surcharge. Ainsi, le prestataire doit s'assurer que les ressources allouées aux différents utilisateurs du service sont suffisantes pour couvrir les besoins.	x			Système d'accès / Système du prestataire / Système d'accès du prestataire
10	10.5 Sauvegarde	Sauvegarde des informations - backups	Le prestataire doit prendre toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé. Il doit notamment effectuer un double exemplaire des sauvegardes et doit les conserver dans des locaux physiquement séparés.	x	x	x	Système du prestataire
11	10.10 Surveillance	Protection des informations journalisées	Protection des équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés. Analyser les journaux à l'aide d'un logiciel de contrôle de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
12	10.10 Surveillance	Journal administrateur et journal des opérations	La journalisation des opérations des administrateurs permet de garder une trace des actions des administrateurs.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
13	10.10 Surveillance	Rapports de défaut	Journaliser et analyser les éventuels défauts et prendre les mesures appropriées.		x	x	Système d'accès / Système du prestataire / Système d'accès du prestataire
14	10.10 Surveillance	Audit de la passerelle d'accès au cloud	La passerelle d'accès au cloud doit être soumise à un audit régulier (annuel) pour vérifier que les mesures de sécurité sont effectives et en adéquation avec les objectifs de sécurité.	x			Système d'accès
15	11.4 Contrôle d'accès au réseau	Protection des ports de diagnostic et de configuration à distance	Le prestataire doit contrôler l'accès physique et logique aux ports de diagnostic et de configuration à distance.	x	x		Système du prestataire / Système d'accès du prestataire
16	11.4 Contrôle d'accès au réseau	Mesure relative à la connexion réseau	Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme du prestataire, il convient de vérifier que le prestataire restreigne la capacité de connexion réseau des utilisateurs, conformément à la politique de contrôle d'accès et les exigences relatives aux applications de gestion.	x	x		Système d'accès du prestataire
17	11.4 Contrôle d'accès au réseau	Contrôle du routage réseau interne	S'assurer que l'organisation mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		Système d'accès
18	11.4 Contrôle d'accès au réseau	Contrôle du routage réseau du prestataire	S'assurer que le prestataire mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		Système d'accès du prestataire
22	12.6 Gestion des vulnérabilités techniques	Mesures relatives aux vulnérabilités techniques	Le prestataire doit tenir informé l'organisation (assureur) en temps voulu de toute vulnérabilité technique des systèmes d'information en exploitation, évaluer l'exposition de l'organisation auxdites vulnérabilités et entreprendre les actions appropriées pour traiter le risque associé. Cette démarche doit être formalisée dans le contrat de service.	x			Système du prestataire
24		Hébergement non mutualisé	L'hébergement doit être réalisé sur une ou plusieurs machines spécifiques (non mutualisé). Ainsi, les données de l'organisation (assureur) ne risquent pas de subir les conséquences d'une activité frauduleuse d'un autre client du cloud. Les problèmes de compartimentation sont de plus écartés.	x			Système du prestataire
25	15.1 Conformité avec les exigences légales	Localisation des données	Le prestataire doit être en mesure d'indiquer la localisation des données pour informer l'organisation	x			Système du prestataire

Niveau de risque après application des mesures de sécurité complémentaires

Niveau de risque	**1. Négligeable**	~~2. Limité~~	3. Significatif	4. Intolérable

Gravité	**1. Négligeable**	~~2. Limitée~~	3. Importante	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

4.1.7 Divulgation de la fonction de traitement des données de déclaration de sinistre

La divulgation de la fonction de traitement est considérée comme insignifiante dans le contexte de cette étude. Le risque n'est donc pas considéré.

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Traitement des données					
ER7	Divulgation de la fonction de traitement	Réservé	• Employé malveillant • Employé du prestataire malveillant • Pirate	• Perte d'un avantage concurrentiel	**0. Insignifiant**

4.1.8 Dysfonctionnement de la fonction de traitement des données de déclaration de sinistre

L'altération de la fonction de traitement est considérée comme insignifiante dans le contexte de cette étude. Le risque n'est donc pas considéré.

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Traitement des données					
ER8	Altération de la fonction de traitement	Intègre	• Employé malveillant • Employé du prestataire malveillant • Pirate	• Traitement des données non valide • Perte de confiance vis-à-vis des clients • Perte de notoriété • Perte de crédibilité	**0. Insignifiant**

4.1.9 Arrêt de la fonction de traitement des données de déclaration de sinistre

Scénarios décrits dans les documents (ANSSI et ENISA)

Bien(s) support(s)	Scénario(s) de menace
Système du prestataire – Logiciel d'administration du prestataire	Le Cloud Provider a mal estimé les ressources à allouer et provoque une indisponibilité du système d'information.
Système d'accès du prestataire – Réseau du prestataire	Une panne dans le réseau du prestataire empêche l'accès au cloud.
Système d'accès du prestataire – Réseau du prestataire	Un employé malveillant provoque une perte de liaison entre les serveurs du prestataire et empêche l'accès au cloud.
Système du prestataire – Logiciel d'administration du prestataire	Le Cloud Provider fait faillite alors que la portabilité des données, des applications et des services n'est pas assurée.
Système d'accès – Réseau internet	Un pirate, un concurrent ou un employé souhaitant se venger provoque un déni de service empêchant l'accès au cloud.
Système d'accès – Réseau internet	Une panne de réseau empêche l'accès au cloud.

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Traitement des données					
ER9	Indisponibilité de la fonction de traitement	24h	• Mauvaise gestion du prestataire • Pirate • Concurrent • Employé malveillant • Panne de réseau	• Impossibilité d'assurer le traitement • Perte de confiance vis-à-vis des clients • Perte de notoriété	3. Importante

Résultat obtenu par le logiciel

Bien support	Scénarios de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système du prestataire (SYS_EXT)	Menace sur le système du prestataire causant une indisponibilité	D	• Employé du prestataire peu sérieux • Employé du prestataire malveillant • Décision du cloud provider • Concurrent • Pirate • Hébergeur/Faille dans l'application • Décision de justice • Panne de matériel • Bogue logiciel • Catastrophe naturelle	• M9 LOG-DEP Dépassement des limites d'un logiciel • M12 LOG-PTE Disparition d'un logiciel • M6 MAT-PTE Perte d'un matériel • M7 LOG-USG Détournement de l'usage prévu d'un logiciel • M4 MAT-PTE Détérioration d'un matériel • M11 LOG-MOD Modification d'un logiciel	• Surexploitation du système du prestataire • Cessation d'activité du prestataire • Serveurs du prestataire saisis par la justice • Perte ou effacement des données • Changement des données du portail d'accès au cloud	3. Forte

Menace	Vulnérabilités	Pré-requis	Vraisemblance
Surexploitation du système du prestataire	• Manque de compétence du personnel du prestataire • Négligence du personnel du prestataire	• Ressources allouées par le prestataire insuffisantes	1. Minime
Cessation d'activité du prestataire	• Portabilité des données non assurée	• Fébrilité économique du prestataire	2. Significative
Serveurs du prestataire saisis par la justice	• Juridiction liée à la position géographique des données	• Changement de juridiction dans le pays où sont situés les serveurs Ou • Une entreprise tierce mène des activités frauduleuses sur le cloud Ou • Juridiction relative au stockage des données personnelles	2. Significative
Perte ou effacement des données	• Données accessibles avec les droits adéquats • Matériel peu fiable • Matériel inapproprié aux conditions d'utilisation	• Privilèges élevés sur l'application Ou • Contrôle insuffisant du matériel Ou • Bogue dans le logiciel utilisé	3. Forte

	• Datacenter mal protégé contre les catastrophes naturelles • Mauvaise compartimentation du logiciel	Ou • Datacenter dans une zone à risque de catastrophes naturelles Ou • Serveurs partagés (cloud public)	
Changement des données du portail d'accès au cloud	• Données du portail d'accès modifiables • Données du portail d'accès accessibles avec les droits adéquats	• Accès physique ou logique au portail d'accès • Connaissance de l'existence du portail d'accès	3. Forte

Niveau de risque avant application des mesures

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	2. Significative	**3. Forte**	4. Maximale

Mesures de sécurité existantes

N°	Thème ISO 27002	Mesures de sécurité existantes	Description	Prévention	Protection	Récupération	Bien support
1	9.1 Zones sécurisée	Périmètre de sécurité physique	Protéger les zones contenant des informations et des moyens de traitement de l'information par des périmètres de sécurité. Les serveurs doivent être inaccessibles par des personnes non autorisées et donc dans des salles hautement sécurisées.	x	x		Système du prestataire
2	9.1 Zones sécurisée	Contrôle physique des accès	Protéger les zones sécurisées pas des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité soit admis. Le prestataire doit donc surveiller et contrôler les accès aux datacenters et doit s'assurer que le personnel de maintenance ou de support ne peut menacer la sécurité des données, des matériels ou des logiciels.	X	x		Système du prestataire
3	9.1 Zones sécurisée	Protection contre les menaces extérieures et environnementales	Concevoir et appliquer des mesures de protection physiques contre les dommages causés par les incendies, les inondations, les tremblements de terre, les explosions, les troubles civils et autres formes de catastrophes naturelles ou de sinistre provoqués par l'homme. Les datacenters du prestataire devront satisfaire les exigences de sécurité liées à la protection physique des serveurs.	x	X		Système du prestataire
4	9.2 Sécurité du matériel	Services généraux	Protéger le matériel des coupures de courant et autres perturbations dues à une défaillance de services généraux.	x	x	x	Système du prestataire
5	9.2 Sécurité du matériel	Sécurité du câblage	Protéger les câbles électriques ou de télécommunications transportant des données contre toute interception ou dommage.		x		Système d'accès du prestataire
6	10.7 Manipulation des supports	Sécurité de la documentation système	La documentation décrivant l'ensemble du système doit être gardée avec un niveau de sécurité suffisant pour ne pas permettre à des personnes malveillantes d'avoir une connaissance poussée de l'architecture (mesures de « diffusion restreinte » systématiques).		x		Organisation interne / Organisation du prestataire
7	11.2 Gestion de l'accès utilisateur	Gestion des privilèges	Restreindre et contrôler l'attribution et l'utilisation des privilèges (gestion des habilitations).	x	x		Organisation interne
8	11.2 Gestion de l'accès utilisateur	Enregistrement des utilisateurs	Définir une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à accorder et à supprimer l'accès au cloud ou à son administration.	x	x		Organisation interne
9	11.2 Gestion de l'accès utilisateur	Gestion du mot de passe utilisateur	L'attribution de mots de passe doit être réalisée dans le cadre d'un processus formel.		x		Organisation interne / Système d'accès
10	11.3 Responsabilités utilisateurs	Utilisation du mot de passe	Demander aux utilisateurs de respecter les bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe.	x	x		Organisation interne / Système d'accès
11	11.4 Contrôle d'accès au réseau	Authentification des administrateurs	Afin d'accéder aux fonctions d'administration, les administrateurs doivent être authentifiés. L'authentification doit se faire de manière sécurisée (chiffrage des mots de passe, authentification à deux facteurs).		x		Système du prestataire
12	11.4 Contrôle d'accès au réseau	Authentification des utilisateurs	L'authentification des utilisateurs doit se faire de manière sécurisée par un cryptage des mots de passe et une authentification à deux facteurs.		x		Système du prestataire
13	14.1 Aspects de la sécurité de l'information en matière de gestion de l'activité	Plan de continuité de l'activité du prestataire	Le prestataire doit fournir les garanties de continuité de l'activité au travers d'un plan de continuité de l'activité. Ce PCA doit prendre en compte les exigences en matière de sécurité de l'information, les évènements pouvant être à l'origine d'interruption des processus métier, les mesures de restauration et de maintien de la disponibilité du système d'information, ainsi que la mise à l'essai dudit plan de continuité de l'activité.	x		x	Système du prestataire

Niveau de risque après application des mesures de sécurité existantes

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable

Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

Mesures de sécurité complémentaires

N°	Thème ISO 27002	Mesures de sécurité	Description	Prévention	Protection	Récupération	Bien support
2	8.2 Pendant la durée du contrat	Sensibilisation, qualification et formations en matière de sécurité de l'information	Le personnel interne doit être formé aux bonnes pratiques de sécurité. Il doit avoir un niveau de sensibilisation pertinent pour ses fonctions. Cela passe par des sessions de formation et des missives d'information concernant la sécurité.	x	x		Organisation interne
3	8.2 Pendant la durée du contrat	Procédures disciplinaires	Mettre en place un processus disciplinaire clair pour toute ayant enfreint les règles de sécurité pour réduire les risques d'influence et de corruption. Par exemple, les sanctions peuvent être précisées dans une charte définissant les engagements de responsabilités.	x	x		Organisation interne
4	8.3 Fin ou modification de contrat	Retrait des droits d'accès	Les droits d'accès de tout utilisateur ou administrateur aux données et aux logiciels doivent être supprimés en fin de contrat ou doivent être modifiés en cas de changement de contrat ou de responsabilités.	x			Organisation interne
6	10.2 Gestion de la prestation de service par un tiers	Prestation de service et contrat	S'assurer que les mesures de sécurité, les définitions du service et les niveaux de prestation prévus dans l'accord de prestation de service tiers sont mis en œuvre, appliqués et tenus à jour par le tiers. Notamment, le contrat de prestation de service doit inclure les éléments liés à la journalisation d'évènements, au suivi du service hébergé (mise à jour, maintenances, sauvegardes…), aux modalités de prévention d'une attaque et à la réaction suite à un incident.				Système du prestataire
7	10.2 Gestion de la prestation de service par un tiers	Clause contractuelle de restitution des données	Le contrat de prestation de service doit préciser les conditions de restitution des données (conditions, délais, formats) pour permettre le rapatriement des données ou le changement de prestataire sans interruption de service.	x		x	Système du prestataire
9	10.3 Planification et acceptation du système	Dimensionnement	Les ressources doivent correspondre aux besoins. Il est nécessaire de faire des projections et des tests de performance pour connaître les limites du système et pouvoir anticiper toute surcharge. Ainsi, le prestataire doit s'assurer que les ressources allouées aux différents utilisateurs du service sont suffisantes pour couvrir les besoins.	x			Système d'accès / Système du prestataire / Système d'accès du prestataire
10	10.5 Sauvegarde	Sauvegarde des informations - backups	Le prestataire doit prendre toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé. Il doit notamment effectuer un double exemplaire des sauvegardes et doit les conserver dans des locaux physiquement séparés.	x	x	x	Système du prestataire
11	10.10 Surveillance	Protection des informations journalisées	Protection des équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés. Analyser les journaux à l'aide d'un logiciel de contrôle de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
12	10.10 Surveillance	Journal administrateur et journal des opérations	La journalisation des opérations des administrateurs permet de garder une trace des actions des administrateurs.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
13	10.10 Surveillance	Rapports de défaut	Journaliser et analyser les éventuels défauts et prendre les mesures appropriées.		x	x	Système d'accès / Système du prestataire / Système d'accès du prestataire
22	12.6 Gestion des vulnérabilités techniques	Mesures relatives aux vulnérabilités techniques	Le prestataire doit tenir informé l'organisation (assureur) en temps voulu de toute vulnérabilité technique des systèmes d'information en exploitation, évaluer l'exposition de l'organisation auxdites vulnérabilités et entreprendre les actions appropriées pour traiter le risque associé. Cette démarche doit être formalisée dans le contrat de service.	x			Système du prestataire
24		Hébergement non mutualisé	L'hébergement doit être réalisé sur une ou plusieurs machines spécifiques (non mutualisé). Ainsi, les données de l'organisation (assureur) ne risquent pas de subir les conséquences d'une activité frauduleuse d'un autre client du cloud. Les problèmes de compartimentation sont de plus écartés.	x			Système du prestataire
25	15.1 Conformité avec les exigences légales	Localisation des données	Le prestataire doit être en mesure d'indiquer la localisation des données pour informer l'organisation	x			Système du prestataire

Niveau de risque après application des mesures de sécurité complémentaires

Niveau de risque	**1. Négligeable**	~~2. Limité~~	3. Significatif	4. Intolérable
Gravité	**1. Négligeable**	~~2. Limitée~~	3. Importante	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

4.2 Identification des objectifs de sécurité

L'assureur décide de réduire tous les risques jugés comme significatifs ou intolérables. Tous les risques ont au moins le niveau de gravité significatif et ils seront donc tous réduits.

Le tableau suivant présente les objectifs de sécurité identifiés :

Risque	Evitement	Réduction	Prise	Transfert
Divulgation des données de déclaration de sinistre		x		
Altération des données de déclaration de sinistre		x		
Indisponibilité des données de déclaration de sinistre		x		
Divulgation des données de sécurité		x		
Altération des données de sécurité		x		
Indisponibilité des données de sécurité		x		
Indisponibilité de la fonction de traitement des données de déclaration de sinistre		x		

4.3 Identification des risques résiduels

A l'issue de l'identification des objectifs de sécurité, l'organisation a mis en évidence les risques résiduels suivants :

Risques résiduels	Gravité	Vraisemblance
Divulgation des données de déclaration de sinistre	2. Significatif	2. Significatif
Altération des données de déclaration de sinistre	2. Significatif	2. Significatif
Indisponibilité des données de déclaration de sinistre	3. Forte	3. Forte
Divulgation des données de sécurité	2. Significatif	2. Significatif
Altération des données de sécurité	2. Significatif	2. Significatif
Indisponibilité des données de sécurité	2. Significatif	3. Forte
Indisponibilité de la fonction de traitement des données de déclaration de sinistre	3. Forte	3. Forte

5 Module 5 - Étude des mesures de sécurité

5.1 Définition des mesures de sécurité

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	6.1 Organisation interne	Attribution des responsabilités en matière de sécurité de l'information	Il convient de définir clairement toutes les responsabilités en matière de sécurité de l'information. La répartition des responsabilités entre le personnel interne et le personnel du prestataire doit être formalisée et respectée.	x			Organisation interne / Organisation externe
2	8.2 Pendant la durée du contrat	Sensibilisation, qualification et formations en matière de sécurité de l'information	Le personnel interne doit être formé aux bonnes pratiques de sécurité. Il doit avoir un niveau de sensibilisation pertinent pour ses fonctions. Cela passe par des sessions de formation et des missives d'information concernant la sécurité.	x	x		Organisation interne
3	8.2 Pendant la durée du contrat	Procédures disciplinaires	Mettre en place un processus disciplinaire clair pour toute ayant enfreint les règles de sécurité pour réduire les risques d'influence et de corruption. Par exemple, les sanctions peuvent être précisées dans une charte définissant les engagements de responsabilités.	x	x		Organisation interne
4	8.3 Fin ou modification de contrat	Retrait des droits d'accès	Les droits d'accès de tout utilisateur ou administrateur aux données et aux logiciels doivent être supprimés en fin de contrat ou doivent être modifiés en cas de changement de contrat ou de responsabilités.	x			Organisation interne
5	9.2 Sécurité du matériel	Mise au rebut ou recyclage sécurisé du matériel	Vérifier tout le matériel contenant des supports de stockage pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut. Le prestataire devra préciser les mesures mises en œuvre pour assurer la mise au rebut de ses matériels.	x	x		Système du prestataire
6	10.2 Gestion de la prestation de service par un tiers	Prestation de service et contrat	S'assurer que les mesures de sécurité, les définitions du service et les niveaux de prestation prévus dans l'accord de prestation de service tiers sont mis en œuvre, appliqués et tenus à jour par le tiers. Notamment, le contrat de prestation de service doit inclure les éléments liés à la journalisation d'évènements, au suivi du service hébergé (mise à jour, maintenances, sauvegardes…), aux modalités de prévention				Système du prestataire

			d'une attaque et à la réaction suite à un incident.				
7	10.2 Gestion de la prestation de service par un tiers	Clause contractuelle de restitution des données	Le contrat de prestation de service doit préciser les conditions de restitution des données (conditions, délais, formats) pour permettre le rapatriement des données ou le changement de prestataire sans interruption de service.	x		x	Système du prestataire
8	10.2 Gestion de la prestation de service par un tiers	Gestion des modifications dans les services tiers	Gérer les changements effectués dans la prestation de service, comprenant le maintien et l'amélioration des politiques, procédures et mesures existantes. Notamment, le contrat doit permettre la validation des choix du prestataire lors de la mise en œuvre de nouvelles solutions logicielles ou matérielles (pour éviter la perte de sécurité).	x	x		Système du prestataire
9	10.3 Planification et acceptation du système	Dimensionnement	Les ressources doivent correspondre aux besoins. Il est nécessaire de faire des projections et des tests de performance pour connaître les limites du système et pouvoir anticiper toute surcharge. Ainsi, le prestataire doit s'assurer que les ressources allouées aux différents utilisateurs du service sont suffisantes pour couvrir les besoins.	x			Système d'accès / Système du prestataire / Système d'accès du prestataire
10	10.5 Sauvegarde	Sauvegarde des informations - backups	Le prestataire doit prendre toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé. Il doit notamment effectuer un double exemplaire des sauvegardes et doit les conserver dans des locaux physiquement séparés.	x	x	x	Système du prestataire
11	10.10 Surveillance	Protection des informations journalisées	Protection des équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés. Analyser les journaux à l'aide d'un logiciel de contrôle de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
12	10.10 Surveillance	Journal administrateur et journal des opérations	La journalisation des opérations des administrateurs permet de garder une trace des actions des administrateurs.	x	x		Système d'accès / Système du prestataire / Système d'accès du prestataire
13	10.10 Surveillance	Rapports de défaut	Journaliser et analyser les éventuels défauts et prendre les mesures appropriées.		x	x	Système d'accès / Système du prestataire / Système d'accès du prestataire
14	10.10 Surveillance	Audit de la passerelle d'accès au cloud	La passerelle d'accès au cloud doit être soumise à un audit régulier (annuel) pour vérifier que les mesures de sécurité sont effectives et en adéquation avec les objectifs de sécurité.	x			Système d'accès
15	11.4 Contrôle d'accès au réseau	Protection des ports de diagnostic et de configuration à distance	Le prestataire doit contrôler l'accès physique et logique aux ports de diagnostic et de configuration à distance.	x	x		Système du prestataire / Système d'accès

							du prestataire
16	11.4 Contrôle d'accès au réseau	Mesure relative à la connexion réseau	Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme du prestataire, il convient de vérifier que le prestataire restreigne la capacité de connexion réseau des utilisateurs, conformément à la politique de contrôle d'accès et les exigences relatives aux applications de gestion.	x	x		Système d'accès du prestataire
17	11.4 Contrôle d'accès au réseau	Contrôle du routage réseau interne	S'assurer que l'organisation mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		Système d'accès
18	11.4 Contrôle d'accès au réseau	Contrôle du routage réseau du prestataire	S'assurer que le prestataire mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		Système d'accès du prestataire
19	12.3 Mesures cryptographiques	Politique d'utilisation des mesures cryptographiques	Elaboration et mise en œuvre d'une politique d'utilisation des mesures cryptographiques en vue de protéger l'information. Par exemple, employer un logiciel de chiffrement des données externalisées.	x			Système du prestataire
20	12.3 Mesures cryptographiques	Chiffrement des flux	Les flux contenant des informations sensibles ou à caractère personnel doivent être chiffrées.	x			Système d'accès
21	12.3 Mesures cryptographiques	Gestion des clés	Une procédure de gestion des clés doit venir à l'appui de la politique de l'organisme en matière de chiffrement.	x			Système du prestataire / Système d'accès
22	12.6 Gestion des vulnérabilités techniques	Mesures relatives aux vulnérabilités techniques	Le prestataire doit tenir informé l'organisation (assureur) en temps voulu de toute vulnérabilité technique des systèmes d'information en exploitation, évaluer l'exposition de l'organisation auxdites vulnérabilités et entreprendre les actions appropriées pour traiter le risque associé. Cette démarche doit être formalisée dans le contrat de service.	x			Système du prestataire
23	15.1 Conformité avec les exigences légales	Protection des données et confidentialité des informations relatives à la vie privée	Le prestataire doit satisfaire les exigences de protection et de confidentialité des données à caractère personnel telles que l'exigent la législation ou les réglementations applicables. Le transfert des données à caractère personnel en dehors des frontières de l'Union européenne est réglementé par la directive européenne 95/46/CE et la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.		x		Système du prestataire
24		Hébergement non mutualisé	L'hébergement doit être réalisé sur une ou plusieurs machines spécifiques (non mutualisé). Ainsi, les données de l'organisation (assureur) ne risquent pas de subir les conséquences d'une activité frauduleuse d'un autre client du cloud. Les problèmes de compartimentation sont de plus écartés.	x			Système du prestataire
25	15.1 Conformité avec les exigences légales	Localisation des données	Le prestataire doit être en mesure d'indiquer la localisation des données pour informer l'organisation	x			Système du prestataire

5.2 Analyse des risque résiduels

Divulgation des données de déclaration de sinistre

Niveau de risque	**1. Négligeable**	2. Limité	~~3. Significatif~~	4. Intolérable
Gravité	**1. Négligeable**	2. Limitée	~~3. Importante~~	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

Altération des données de déclaration de sinistre

Niveau de risque	**1. Négligeable**	2. Limité	~~3. Significatif~~	4. Intolérable
Gravité	**1. Négligeable**	2. Limitée	~~3. Importante~~	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

Indisponibilité des données de déclaration de sinistre

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

Divulgation des données de sécurité

Niveau de risque	1. Négligeable	**2. Limité**	3. Significatif	~~4. Intolérable~~
Gravité	1. Négligeable	**2. Limitée**	3. Importante	~~4. Critique~~
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

Altération des données de sécurité

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

Indisponibilité des données de sécurité

Niveau de risque	**1. Négligeable**	~~2. Limité~~	3. Significatif	4. Intolérable
Gravité	**1. Négligeable**	~~2. Limitée~~	3. Importante	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

Arrêt de la fonction de traitement des données de déclaration de sinistre

Niveau de risque	**1. Négligeable**	~~2. Limité~~	3. Significatif	4. Intolérable
Gravité	**1. Négligeable**	~~2. Limitée~~	3. Importante	4. Critique

Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

5.3 Déclaration d'applicabilité

Ce point sera à complété avec le logiciel.

5.4 Mise en œuvre des mesures de sécurité

Ce point sera à complété avec le logiciel.

Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Sous-direction assistance, conseil et expertise
Bureau assistance et conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
ebios@ssi.gouv.fr

Identification de la contribution
Nom et organisme (facultatif) : .....
Adresse électronique : .....
Date : .....

Remarques générales sur le document
Le document répond-il à vos besoins ? Oui ☐ Non ☐

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui ☐ Non ☐

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?
.....
.....

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?
.....
.....

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui ☐ Non ☐

Si oui :

Dans quel domaine peut-on l'améliorer ?
- lisibilité, compréhension ☐
- présentation ☐
- autre ☐

Précisez vos souhaits quant à la forme :
.....
.....

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :
.....
.....

Quels autres sujets souhaiteriez-vous voir traiter ?
.....
.....

Remarques particulières sur le document

Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne…).

"Énoncé de la remarque" permet de formaliser le commentaire.

"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

N°	Type	Référence	Énoncé de la remarque	Solution proposée
1				
2				
3				
4				
5				

Merci de votre contribution